DES-7200

Basic Configuration Command Reference Guide

Version 10.4(3)

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 CLI Authorization Configuration Commands

1.1 alias

You can use the **alias** command to configure an alias of a command in the global configuration mode. Use the **no** form of the command to remove the alias of a specified command or all the aliases under one mode.

alias *mode command-alias original-command*

no alias *mode command-alias*

Parameter description

Parameter	Description
mode	Mode of the command represented by the alias
command-alias	Alias of the command
original-command	Syntax of the command represented by the alias

Default Settings

Some commands in the privileged EXEC mode have default alias names.

Command mode

Global configuration mode.

Usage guidelines

The following table lists the default alias of the commands in the privileged EXEC mode.

Alias	Actual Command
h	**help**
p	**ping**
s	**show**

un	**undebug**

The default alias cannot be deleted by the **no alias exec** command.

By setting the alias, you can use a word to replace a command. For example, you can create an alias to represent the first part of a command, and then type the rest part of the command.

The mode of the command represented by the alias is the command mode existing in the current system. In the global configuration mode, you can use **alias ?** to list all the modes under which you can configure alias for commands.

```
DES-7200(config)# alias ?
  aaa-gs              AAA server group mode
  acl                 acl configure mode
  bgp                 Configure bgp Protocol
  config              globle configure mode
.......
```

The alias also has its help information that is displayed after * in the following format:

**command-alias=original-command*

For example, in the privileged EXEC mode, the default alias **s** stands for **show**. You can enter **s?** to query the key words beginning with **s** and the help information of the alias.

```
DES-7200#s?
*s=show  show  start-chat  start-terminal-service
```

If an alias represents more than one word, the command will be displayed in brackets. For example, if you set **sv** stand for **show version** in the privileged EXEC mode, then:

```
DES-7200#s?
*s=show  *sv="show version" show  start-chat
start-terminal-service
```

The alias must begin with the first letter of the command. The first letter of the command cannot be a space. The space before the command cannot be used as a valid alias.

```
DES-7200# s?
show  start-chat  start-terminal-service
```

The command alias also has its help information. For example, if the alias **ia** represents **ip address** in the

interface configuration mode, then:

```
DES-7200(config-if)#ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
DES-7200(config-if)# ip address
```

The above help information lists the parameters of **ip address** and shows the actual command name.

You must enter an entire alias; otherwise it cannot be recognized.

Use the **show aliases** command to show the aliases setting in the system.

Examples

In the global configuration mode, use **def-route** to represent the default route setting of **ip route 0.0.0.0 0.0.0.0 192.168.1.1:**

```
DES-7200# configure terminal
DES-7200(config)# alias config def-route ip route 0.0.0.0
0.0.0.0 192.168.1.1
DES-7200(config)#def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
DES-7200(config)# end
DES-7200# show aliases config
globle configure mode alias:
def-route          ip route 0.0.0.0 0.0.0.0
192.168.1.1
```

Related commands

Command	Description
show aliases	Show the aliases settings.

1.2 privilege

To attribute the execution rights of a command to a command level, use **privilege** in the global configuration mode. The **no** form of this command recovers the execution rights of a command to the default setting.

privilege *mode* [**all**] [**level** *level* **| reset**] *command-string*

no privilege *mode* [**all**] [**level** *level*] *command-string*

Parameter description

Parameter	Description
mode	CLI mode of the command to which the execution rights are attributed.
all	Alias of the command
level	Specify the execution right levels

	(0–15) of a command or sub-commands
reset	Restore the command execution rights to its default level
command-string:	Command string to be authorized

Default Settings

N/A.

Command mode

Global configuration mode.

Usage guidelines

The following table lists some key words that can be authorized by command **privilege** in the CLI mode. The number of command modes that can be authorized may vary with different devices. In the global configuration mode, you can use **privilege ?** to list all CLI command modes that can be authorized.

Mode	Descripton
config	Global configuration mode.
exec	Privileged EXEC mode
interface	Interface configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
keychain	KeyChain configuration mode
keychain-key	KeyChain-key configuration mode
time-range	Time-Range configuration mode

Examples

Set the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

```
DES-7200(config)#enable secret level 1 0 test
DES-7200(config)#privilege exec level 1 reload
```

After the above setting, you can access the CLI window as level-1 user to use the **reload** command:

```
DES-7200>reload ?
  LINE   Reason for reload
```

```
  <cr>
```

You can use the key word **all** to attribute all sub-commands of reload to level-1 users:

```
DES-7200(config)# privilege exec all level 1 reload
```

After the above setting, you can access the CLI window as level-1 user to use all sub commands of the **reload** command:

```
DES-7200>reload ?
  LINE    Reason for reload
  at                  reload at a specific time/date
  cancel              cancel pending reload scheme
  in                  reload after a time interval
<cr>
```

Related commands

Command	Description
enable secret	Set CLI-level password

1.3 show aliases

To display all the command aliases or aliases in special command modes, run the **show aliases** command in the privileged EXEC mode.

show aliases [*mode***]**

Parameter description

Parameter	Description
mode	Mode of the command represented by the alias.

Default Settings

N/A.

Command mode

EXEC mode.

Usage guidelines

Show all the configuration of aliases if the command mode has not been input.

Examples

Following example shows the command alias in the EXEC mode:

```
DES-7200#show aliases exec
```

```
exec mode alias:
h                 help
p                 ping
s                 show
u                 undebug
un                undebug
```

Related commands

Command	Description
alias	Set the alias of a command.

2 Switch Management Configuration Commands

2.1 User Management Related Commands

2.1.1 disable

To exit from privileged user mode to normal user mode or lower the privilege level, execute the privileged user command **disable**.

disable [*privilege-level*]

Parameter description

Parameter	Description
privilege-level	Privilege level

Command mode

Privileged mode.

Usage guidelines

Use this command to return to user mode from privileged mode. If a privilege level is added, the current privilege level will be lowered to the specified level.

Note The privilege level following the **disable** command must be lower than the current level.

Examples

The example below lowers the current privilege level of the device down to level 10:

```
DES-7200# disable 10
```

Related commands

Command	Description
enable	From user mode enter to the privileged mode or log on the higher level of authority.

2.1.2 enable

To enter into the privileged user mode, execute the normal user configuration command **enable**.

For the details of the command, see the *Security Configuration Command Reference*.

2.1.3 enable password

To configure the password for different privilege level, execute the global configuration command **enable password**. The **no** form of this command is used to delete the password of the specified level.

enable password [**level** *level*] {*password* | [**0**|**7**] *encrypted-password*}

no enable password [**level** *level*]

Parameter description

Parameter	Description
Password	Password for user to enter into the EXEC configuration layer
Level	User's level.
0|7	Password encryption type, "0" for no encryption, "7" for simple encryption
encrypted-password	Password text.

Command mode Global configuration mode.

Usage guidelines

No encryption is required in general. The encryption type is required generally when the password that has been encrypted with the command for the device are to be copies and pasted.

The effective password is defined as below:

- Consists of 1 ~ 26 letter in upeer/lower case and numerals
- Leading spaces are allowed but ignored. Spaces in between or at the end are regarded as part of the password.

Caution

If an encryption type is specified and then a plaintext password is entered, it is impossible to enter into the privileged EXEC mode. A lost password that has been encrypted with any method cannot be restored. The only way is to reconfigure the device password.

Examples

The example below configures the password as **pw10**:

```
DES-7200(config)# enable password pw10
```

Related commands

Command	Description
enable secret	Set the security password

2.1.4 enable secret

To configure the security password for different privilege level, execute the global configuration command **enable secret**. The **no** form of this command is used to delete the password of the specified level.

enable secret [**level** *level*] {*secret* | [**0|5**] *encrypted-secret*}

no enable secret

Parameter description

Parameter	Description
secret	Password for user to enter into the EXEC configuration layer
level	User's level.
0|5	Password encryption type, "0" for no encryption, "5" for security encryption
encrypted-password	Password text

Command mode	Global configuration mode.
Usage guidelines	The password falls into "password" and "security" passwords. The "password" is simple encryption password, which can be set only for level 15. The "security" means the security encryption password, which can be set for level 0 ~ 15. If the two kinds of passwords exist in the system at the same time, the "password" type password will not take effect. If a "password" type password is set for a level other than 15, an alert is provided and the password is automatically converted into the "security" password. If "password" type password is set for level 15 and the same as the "security" password, an alert is provided. The password must be saved in encrypted manner, with simple encryption for the "password" type password and security encryption for the "security" type password.
Examples	The example below configures the security password as pw10: `DES-7200(config)# enable secret 0 pw10`

Related commands

Command	Description
enable password	Set passwords for different privilege levels.

2.1.5 enable service

To enable or disable the specified service such as **SSH Server/Telnet Server/Web Server/SNMP Agent**, use the **enable service** command in the global configuration mode:

enable service { **ssh-sesrver** | **telnet-server** | **web-server** | **snmp-agent**}

Parameter description

Keyword	Description
ssh-server	Enable SSH Server, and the IPv4 and IPv6 services are enabled at the same time.
telnet-server	Enable Telnet Server, and the IPv4 and IPv6 services are enabled at the same time.

	web-server	Enable HTTP Server, and the IPv4 and IPv6 services are enabled at the same time.
	snmp-agent	Enable SNMP Agent, and the IPv4 and IPv6 services are enabled at the same time.

Command mode	Global configuration mode.
Usage guidelines	This command is used to enable the specified service. Use the **no enable service** command to disable the specified service.
Examples	The example below enables the SSH Server: `DES-7200(Config)# enable service ssh-sesrver`

Related commands	**Command**	**Description**
	show service	View the service status of the current system.

2.1.6 execute

To execute the commands in the batch files, use the privileged EXEC mode command **execute**.

execute [**flash:**] *filename*

Parameter description	**Parameter**	**Description**
	flash:	Parent directory of the batch file
	filename	Name of the batch file

Default configuration	N/A
Command mode	Privileged EXEC mode.

Usage guidelines

This command is used to execute the commands in the batch files. Users could self-specify the filename and content of the batch file. In general, after finishing editting the batch files on the user PC , the files are transmit to the Flash of the device through the TFTP. The content of batch files completely imitates the user entering, so the content should be edited in order of CLI command configuration. Besides, for some interactive commands , the response message should be pre-wrote into the batch files to ensure the commands can be normally executed.

Caution: The size of the batch file shall not exceed 128K, otherwise the execution of batch files may fail. For the over-sized batch files, you can divide them into several small files with size less than 128K to complete the execution.

Examples

The example below executes the batch file line_rcms_script.text ,which is used to enable the reverse **Telnet** function for all asynchronous Interfaces, and whose contents are as follows:

```
configure terminal
line tty 1 16
transport input all
no exec
end
```

The execution result is as below:

```
DES-7200# execute flash:line_rcms_script.text
executing script file line_rcms_script.text ......
executing done
DES-7200# configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
DES-7200(config)# line tty 1 16
DES-7200(config-line)# transport input all
DES-7200(config-line)# no exec
DES-7200(config-line)# end
```

2.1.7 ip http authentication

When using the Http Server, it needs to perform the logon authentication to enter the Web page. Use this command to set the mode of Web logon authentication.

ip http authentication {enable | local }

Parameter description	**Keyword**	**Description**
	enable	Use the password set by the **enable password** or **enable secret**, the password must be of the level15.
	local	Use the username and password set by the local **username** command. The user must bind to the privilege of level15.
Default	**enable**	
Command mode	Global configuration mode.	
Usage guidelines	This command is used to set the mode of Web logon authentication. Use the **no ip http authentication** command to restore it to the default setting.	
Examples	The example below sets the mode of Web logon authentication as local: `DES-7200(Config)# ip http authentication local`	
Related commands	**Command**	**Description**
	enable service	Enable or disable the specified service.

2.1.8 ip http port

To set the port of the HTTP service ,use this command in the global configuration mode:

ip http port *number*

Parameter description	**Keyword** / **Description** *number* / Port number of the HTTP server, the default value is 80.
Default configuration	80
Command mode	Global configuration mode.
Usage guidelines	This command is used to set the port of the HTTP service. Use the **no ip http port** command to restore it to the default setting.
Examples	The example below set the port of the HTTP service as 8080: `DES-7200(Config)# ip http port 8080`
Related commands	**Command** / **Description** **enable service** / Enable or disable the specified service

2.1.9 ip http source-port

This command is used to configure the port for HTTPS services in the global configuration mode.

ip http source-port *number*

Parameter description	**Parameter** / **Description** *number* / Configure the port for HTTPS services, and the default value is 443.
Default configuration	443
Command mode	Global configuration mode.

Usage guidelines	This command is used to configure the port for HTTPS services. The no form of this command is used to restore the default port configuration.
Examples	The example below sets the port for HTTPS services as 4443. `DES-7200(config)# ip http secure-port 4443`

Related commands

Command	Description
enable service	Enable or disable the specified service.
show web-server status	Show the status of the web server.

2.1.10 ip telnet source-interface

To specify the IP address of one interface as the source address for the Telnet connection, use the **ip telnet source-interface** command in the global configuration mode:

ip telnet source-interface *interface-name*

Parameter description

Keyword	Description
interface-name	Name of the specified interface

Command mode	Global configuration mode.
Usage guidelines	This command is used to specify the IP address of one interface as the source address for the global Telnet connetction. When using the telnet command to log in a Telnet server, if no source interface or source address is specified for this connnetcion, the global setting is used.Use the **no ip telnet source-interface** command to restore it to the default setting.
Examples	The example below specifies the IP address of the interface *Loopback1* as the source address for the global Telnet connection. `DES-7200(Config)# ip telnet source-interface Loopback 1`

Related commands	**Command**	**Description**
	telnet	log in a Telnet server

2.1.11 lock

To set a temporary password at the terminal, execute the EXEC mode command **lock**.

lock

Parameter description	N/A.
Command mode	Privileged mode.
Usage guidelines	You can lock the terminal interface but maintain the continuity of session, to prevent it from being accessed by setting the temporary password.The terminal interface can be locked by the steps below: 1. Enter the **lock** command, and the system will prompt you to enter the password: 2. Enter the password, which may be any string.The system will prompt you to confirm the entered password, and then clear the screen as well as show the "Locked" information. 3. To enter into the terminal, enter the set temporary password. To use the terminal locked function at the terminal, execute the **lockable** command in the line configuration mode, and enable the characteristic to support the terminal lock in corresponding line.

Examples	The example below locks a terminal interface:
	`DES-7200(config-line)# lockable`
	`DES-7200(config-line)# end`
	`DES-7200# lock`
	`Password: <password>`
	`Again: <password>`
	
	`Locked`
	`Password: <password>`
	`DES-7200#`

Related commands	**Command**	**Description**
	lockable	Set to support the terminal lock function in the line.

2.1.12 lockable

To support the use of the **lock** command at the terminal, execute the **lockable** command in the line configuration mode. The terminal doesn't support the **lock** command, by default.Use the **no** command to cancel the setting.

lockable

no lockable

Parameter description	N/A.
Command mode	Line configuration mode.
Usage guidelines	This command is used to support the terminal lock function in corresponding line. To lock the terminal, execute the **lock** command in the EXEC mode.

Examples

The example below enables the terminal lock function at the console port and locks the console:

```
DES-7200(config)# line console 0
DES-7200(config-line)# lockable
DES-7200(config-line)# end
DES-7200# lock
Password: <password>
Again: <password>

Locked

Password: <password>
DES-7200#
```

Related commands	**Command**	**Description**
	lock	Lock the terminal.

2.1.13 login

In case the AAA is disabled, to enable simple logon password authentication on the interface, execute the interface configuration command **login**. The **no** form of this command is used to delete the line logon password authentication.

login

no login

Parameter description	N/A.
Command mode	Line configuration mode.
Usage guidelines	If the AAA security server is not enabled, this command is used for the simple password authentication at logon. The password here is the one configured for VTY or console interface.

Examples	The example below shows how to set the logon password authentication on VTY.
	`DES-7200(config)# no aaa new-model`
	`DES-7200(config)# line vty 0`
	`DES-7200(config-line)# password 0 normatest`
	`DES-7200(config-line)# login`

Related commands

Command	Description
password	Configure the line logon password

2.1.14 login authentication

In case the AAA is enabled, the authentication with the AAA server must be performed for logon. Use this command to associate logon authentication method list. The **no** form of this command is used to delete the logon authentication method list.

login authentication {**default** | *list-name*}

no login authentication {**default** | *list-name*}

Parameter description

Parameter	Description
default	Name of the default authentication method list
list-name	Name of the method list available

Command mode

Line configuration mode.

Usage guidelines

If the AAA security server is enabled, this command is used for the logon authentication with the specified method list.

Examples

The example below shows how to associate method list on VTY and perform logon authentication with radius.

```
DES-7200(config)# aaa new-model
DES-7200(config)# aaa authentication login default radius
DES-7200(config)# line vty 0
DES-7200(config-line)# login authentication default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service
aaa authentication login	Configure the logon authentication method list

2.1.15 login local

In case the AAA is disabled, to enable local user authentication on the interface, execute the interface configuration command **login local**. The **no** form of this command is used to delete the line local user authentication.

login local

no login local

Parameter description

N/A.

Command mode

Line configuration mode.

Usage guidelines	If the AAA security server is not enabled, this command is used for the local user authentication at logon. The user here means the one configured with the **username** command.

Examples

The example below shows how to set the local user authentication on VTY.

```
DES-7200(config)# no aaa new-model
DES-7200(config)# username  test password 0 test
DES-7200(config)# line vty 0
DES-7200(config-line)# login local
```

Related commands

Command	Description
username	Configure the local user information.

2.1.16 password

To configure the password for line logonexecute the line configuration command **password**. The **no** form of this command is used to delete the line logon password.

password {*password* | [**0**|**7**] *encrypted-password*}

no password

Parameter description

Parameter	Description
password	Password for line of remote user
0|7	Password encryption type, "0" for no encryption, "7" for simple encryption
encrypted-password	Password text

Command mode	Line configuration mode.
Usage guidelines	This command is used to configure the authentication password for the line logon of remote user.

Examples

The example below configures the line logon password as "red":

```
DES-7200(config)# line  vty 0
DES-7200(config-line)# password red
```

Related commands	**Command**	**Description**
	login	From user mode enter to the privileged mode or log on the higher level of authority.

2.1.17 privilege mode

Please refer to the *chapter of configure CLI authorization commands.*

Default configuration	Please refer to the *chapter of configure CLI authorization commands.*
Command mode	Please refer to the *chapter of configure CLI authorization commands.*
Usage guidelines	Please refer to the *chapter of configure CLI authorization commands.*
Examples	Please refer to the *chapter of configure CLI authorization commands.*

2.1.18 service password-encryption

To encrypt the password, execute this command. The **no** form of this command restores to the default value, but the password in cipher text cannot be restored to plain text.

service password-encryption

no service password-encryption

Parameter description	N/A.
Command mode	Global configuration mode.

Usage guidelines	This command is disabled by default. Various passwords are displayed in form of plain text, unless it is directly configured in cipher text form. After you execute the **service password-encryption** and **show running** or **write** command to save the configuration, the password transforms into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.
Examples	The example below encrypts the password: `DES-7200(config)# service password-encryption`

Related commands

Command	Description
enable password	Set passwords of different privileges.

2.1.19 telnet

To log in one server which supports the telnet connection, use the **telnet** command to log on in the EXEC (privileged) mode.

telnet *host* [*port*] [**/source** {**ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name}*] [**/vrf** *vrf-name*]

Parameter description

Parameter	Description
host	The IP address of host or host name to be logged in.
port	Select the TCP port number to be used for the login, 23 by default.
/source	Specify the source IP or source interface used by the Telnet client.
ip *A.B.C.D*	Specify the source IPv4 address used by the Telnet client.
ipv6 *X:X:X:X::X*	Specify the source IPv6 address used by the Telnet client.
interface *interface-name*	Specify the source interface used by the Telnet client.
/vrf *vrf-name*	Specify the VRF routing table to be queried.

Command mode	Privileged mode.

Usage guidelines

This command is used to log in a telnet server.

Caution

The **/ipv6** keyword is only applied to the IPv6 supported devices.

Examples

The example below commands telnet to 192.168.1.11, the port uses the default value, and the source interface is specified as Gi 0/1, the queried VRF route table is specified as vpn1.

```
DES-7200# telnet 192.168.1.11 /source-interface gigabitEthernet 0/1 /vrf vpn1
```

The example below commands telnet to 2AAA:BBBB::CCCC

```
DES-7200# telnet 2AAA:BBBB::CCCC
```

Related commands

Command	Description
Ip telnet source-interface	Specify the IP address of the interface as the source address for the Telnet connection.
show sessions	Show the currently established Telnet sessions.
exit	Exit current connection.

2.1.20 username

To set the local username, execute the global configuration mode command **username**.

username *name* {**nopassword** | **password** { *password* | [**0|7**]

encrypted-password }} **username** *name* **privilege** *privilege-level*

no username *name*

Parameter description

Parameter	Description
name	Username
password	User password
0|7	Password encryption type, 0 for no encryption, 7 for simple encryption
encrypted-password	Password text
privilege-level	User bound privilege level

Command mode	Global configuration mode.
Usage guidelines	This command is used to establish local user database for the purpose of authentication.  **Note** If the type of encryption is specified as 7, the length of the entered legal cipher text should be even. In general, it is not necessary to specify the type of encryption as 7. Commonly, it is necessary to specify the type of encryption as 7 only when the encrypted password is copied and pasted.
Examples	The example below configures a username and password and bind the user to level 15. `DES-7200(config)# username test privilege 15 password 0 pw15`

Related commands

Command	Description
login local	Enable local authentication

2.2 Basic System Management Related Commands

2.2.1 banner login

To configure the login banner, execute the **banner login** command in the global configuration mode. You can use the **no banner login** command to remove the configuration.

banner login *c message c*

Parameter description

Parameter	Description
c	Separator of the message of logging banner. Delimiters are not allowed in the MOTD.
message	Contents of login banner

Command mode	Global configuration mode.
Usage guidelines	This command sets the logging banner message, which is displayed upon login. All characters behind the terminating symbol will be discarded by the system.
Examples	The following example shows the configuration of logging banner: `DES-7200(config)# banner login $ enter your password $`

2.2.2 banner motd

To set the Message-of-the-Day (MOTD), run the **banner motd** command in the global configuration mode. To delete the MOTD setting, run the **no banner motd** command.

banner motd *c message c*

Parameter description

Parameter	Description
c	Separator of the MOTD. Delimiters are not allowed in the MOTD.
message	Contents of an MOTD

Command mode	Global configuration mode.
Usage guidelines	This command sets the MOTD, which is displayed upon login. The letters entered after the separator will be discarded.

Examples	The following example shows the configuration of MOTD:
	`DES-7200(config)`
	`DES-7200(config)# banner motd $ hello,world $`

2.2.3 boot config

This command is used to set the boot configuration filename for the device. The **no** form of this command is used to delete the configured boot configuration filename.

boot config *prefix:/[directory/]filename*

no boot config

Parameter description

Parameter	Description
prefix:	Prefix of file system type. Note that prefix can be used to locate and access files in V10.4(2) or later versions. Refer to *File System Configuration Guide* for details.
/[directory/]filename	File directory and filename

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

This command is used to specify the device's boot configuration filename. When booting the device, the system loads configuration file according to the following principles:

- If the service config command is not configured, the sequence of loading configuration files is as follows: boot configuration filenames configured using the boot config command, flash:/config.text, network boot configuration filenames configured using the boot network command, and the default factory-delivered configuration (null configuration).
- If the service config command is configured, the sequence of loading the configuration file is as follows: network boot configuration filename configured using the boot network command, boot configuration filename configured using the boot config command, flash:/config.text, and the default factory-delivered configuration (null configuration).
- When loading the files in sequence, the system will not load the other configuration files as long as one configuration file is successfully loaded.

This function can be used for fast failure recovery when the device's main configuration file is damaged.

Caution

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

Examples

The following example sets the device's boot configuration filename as "flash:/config_main.text":

```
DES-7200(config)# boot config flash:/config_main.text
```

Related commands

Command	Description
boot network	Set the device's network boot configuration filename.
service config	Allow the device to first download the boot configuration file from a remote network server.
show boot	Show the device's boot configuration.

2.2.4 boot ip

This command is used to configure a local IP for TFTP transmission during device booting. The **no** form of this command is used to delete the configuration.

boot ip *local-ip* [**gateway** *gateway-ip* **mask** *mask-ip*]

no boot ip

Parameter description

Parameter	Description
local-ip	Local IP for TFTP transmission during device booting.
gateway-ip	Gateway IP for TFTP transmission during device booting.
mask-ip	Mask IP for TFTP transmission during device booting.

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

This command is used to configure a local IP for TFTP transmission during device booting. When the device is booting, the system uses this IP as the local IP for TFTP transmission. If a gateway and mask are also configured, and the local IP and gateway IP are not in the same network segment, TFTP uses the gateway for file transmission during system booting.

Caution

Only when the **boot ip** command is correctly configured, can the system download the remote TFTP file configured by the **boot network** or **boot system** command during system booting.

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

Examples	The following example configures a local IP for TFTP transmission during device booting: `DES-7200(config)# boot ip 192.168.7.11`

Related commands	**Command**	**Description**
	show boot	Show the boot related configuration of the device.

2.2.5 boot network

This command is used to set the network boot configuration filename for the divice. The **no** form of this command is used to delete the configured network boot configuration filename.

boot network tftp:// l*ocation* / *filename*

no boot network

Parameter description	**Parameter**	**Description**
	location	Address of the TFTP server.
	filename	Filename on the TFTP server.

Default configuration	None
Command mode	Global configuration mode.

Usage guidelines

This command is used to specify the device's network boot configuration filename. When booting the device, the system loads the configuration file according to the following principles:

- If the service config command is not configured, the sequence of loading the configuration file is as follows: boot configuration filename configured using the boot config command, flash:/config.text, network boot configuration filename configured using the boot network command, and the default factory-delivered configuration (null configuration).
- If the service config command is configured, the sequence of loading the configuration file is as follows: network boot configuration filename configured using the boot network command, boot configuration filename configured using the boot config command, flash:/config.text, and the default factory-delivered configuration (null configuration).
- When loading the files in sequence, the system will not load the other configuration files as long as one configuration file is successfully loaded.

This function can be used for fast failure recovery when the device's master configuration file is damaged accidentally.

Caution

You should use the **boot ip** command to correctly configure the local IP address used by the device during booting, before the system can get the remote file through TFTP. Otherwise any TFTP transmission will fail during booting.

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

Examples

The following example configures the network boot configuration filename for the device:

```
DES-7200(config)# boot network tftp://192.168.7.24/config.text
```

Related

Command	Description

	show boot	Show the boot related configuration of the device.
	boot config	Set the device's boot configuration filename.
	boot ip	Configure the local IP for TFTP transmission during device booting.
	service config	Allow the device to first download the boot configuration file from a remote network server.

2.2.6 boot system

This command is used to set a filename for the device's startup main program and specify the boot priority. The **no** form of this command is used to delete the filename of the main program corresponding to the priority.

boot system *priority* prefix:/[directory/]filename

no boot system [*priority*]

	Parameter	**Description**
Parameter description	*priority*	Boot priority of a main program, in the range of 1 to 10, and 1 is for the highest priority.
	prefix:	Prefix of the file system. Note that prefix can be used to locate and access files in V10.4(2) or later versions. Refer to *File System Configuration Guide* for details.
	/[directory/]filename	Filename of a main program used for booting. Note that when the prefix is used to locate a file, the directory following ":" should be the absolute path.

Default configuration	The default filename of the main boot program is *flash:/firmware.bin*, with the priority being 5.
Command mode	Global configuration mode.

Usage guidelines

This command can be used to set filenames for multiple main programs used for booting and specify the booting priority. The system will attempt to boot the main programs according to their priority levels in the descending order (1 as the top priority and 10 as the lowest priority) during the boot stage. This function can be used for fast failure recovery when the device's main program is damaged.

You should use the **boot ip** command to correctly configure the local IP address used by the device during booting, before the system can get the remote file through TFTP. Otherwise any TFTP transmission will fail during booting. When using TFTP to transmit the boot file, make sure the device's built-in flash has enough space for the boot file. The boot file is saved in the built-in flash as a hidden file during booting and it will be deleted prior to the next booting.

Caution

The **no boot system** *[priority]* command can be used to delete the configured name of the main program corresponding to the boot priority level. If the priority parameter is not set, the configured filenames of all boot main programs will be deleted.

If the **no boot system** command is used to delete all the configured filenames of boot main programs and no filenames of boot main programs are configured, then the system will automatically recover the default configuration (filename of the main program is "flash:/firmware.bin" with the priority level of 5) during the next booting.

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

Examples

Example 1: Configure the name of the main program to “flash:/firmware.bin” and the name of the backup main program to “flash:/ firmware_bak.bin”.

```
DES-7200(config)# boot system 5 flash:/firmware.bin
DES-7200(config)# boot system 8 flash:/firmware_bak.bin
```

As “flash:/firmware.bin” is of a higher priority lever, the device will first boot this file. If “flash:/firmware.bin” is damaged accidentally, which results in booting failure, the system will automatically boot “flash:/firmware_bak.bin” of a lower priority level.

Example 2: Configure to boot the file from a TFTP server.

```
DES-7200(config)# boot system 9 tftp://192.168.7.24/firmware.bin
```

Example 3: Configure to boot the file from a USB drive.

```
DES-7200(config)# boot system 1 usb1:/firmware.bin
```

Example 4: Delete the configured filename of the main program corresponding to priority level 8.

```
DES-7200(config)# no boot system 8
Delete boot system config: [Priority: 8; File Name:
flash:/firmware_bak.bin]? [no] yes
```

Example 5: Delete all configured filenames of boot main programs.

```
DES-7200(config)# no boot system
Clear ALL boot system config? [no] yes
```

Related commands

Command	Description
show boot	Show the boot related configuration of the device.
boot ip	Configure the local IP for TFTP transmission during device booting.

Platform description

N/A

2.2.7 clock set

To configure system clock manually, execute one of the two formats of the privileged user command **clock set**:

clock set *hh:mm:ss month day year*

Parameter description

Parameter	Description
hh:mm:ss	Current time, in the format of Hour (24-hour): Minute: Second
day	Date (1-31) of month
month	Month (1-12) OF year
year	Year (1993-2035), abbreviation is not allowed.

Command mode

Privileged mode.

Usage guidelines

Use this command to set the system time to facilitate the management.

For devices without hardware clock, the time set by the **clock set** command takes effect for only the current setting. Once the device powers off, the manually set time becomes invalid.

Examples

The example below configures the current time as 10:20:30AM March 17th 2003.

```
DES-7200# clock set 10:20:30 Mar 17 2003
DES-7200# show clock
clock: 2003-3-17 10:20:32
```

Related commands

Command	Description
show clock	Show current clock.

2.2.8 clock update-calendar

In the privileged EXEC mode, you can execute command **clock update-calendar** to overwrite the value of hardware clock by software clock.

clock update-calendar

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Some platforms use hardware clock to complement software clock. Since battery enables hardware clock to run continuously, even though the device is closed or restarts, hardware clock still runs. If hardware clock and software clock are asynchronous, then software clock is more accurate. Execute clock update-calendar command to copy date and time of software clock to hardware clock.
Examples	The example below copies the current time and date of software clock to hardware clock: `DES-7200# clock update-calendar`

Related commands

Command	Description
clock read-calendar	Set the softwar clock with the hardware clock value.

2.2.9 exec-timeout

To configure the connection timeout to this equipment in the LINE, use the **exec-timeout** command.Once the connection timeout in the LINE is cancelled by the **no exec-timeout** command, the connection will never be timeout.

exec-timeout *minutes [seconds]*

no exec-timeout

Parameter description

Parameter	Description
minutes	The minutes of specified timeout.
seconds	(optional parameter) The seconds of

		specified timeout.

Default configuration The default timeout is 10min.

Command mode Line configuration mode.

Usage guidelines If there is no input/output information for this connection within specified time, this connection will be interrupted, and this LINE will be restored to the free status.

Examples The example below specifies the connection timeout is 5'30".

```
DES-7200(config-line)#exec-timeout 5 30
```

2.2.10 hostname

To specify or modify the hostname of the device, execute the global configuration command **hostname**.

hostname *name*

Parameter description

Parameter	Description
name	Device hostname, the string, numeral or hyphen are supported only. The maximum length is 63 characters.

Default configuration The default hostname is DES-7200.

Command mode Global Configuration Mode.

Usage guidelines This hostname is mainly used to identify the device and is taken as the username for the local device in the dialup and CHAP authentication.

Examples The example below configures the hostname of the device as BeiJingAgenda:

```
DES-7200(config)# hostname BeiJingAgenda
BeiJingAgenda(config)#
```

2.2.11 prompt

To set the **prompt** command, run the **prompt** command in the global configuration mode. To delete the prompt setting, run the **no prompt** command.

prompt string

Parameter description

Parameter	Description
string	Character string of the **prompt** command. The maximum length is 32 letters.

Command mode

Global configuration mode.

Usage guidelines

If you have not set the prompt string, the prompt string is the system name, which varies with the system name. The **prompt** command is valid only in the EXEC mode.

Examples

Set the prompt string to DES-7210:

```
DES-7200(config)# prompt des-7210
DES-7210(config)# end
DES-7210#
```

2.2.12 reload

To restart the device system, execute the privileged user command **reload**.

reload [*text* | **in** [*hh:*] *mm* [*text*] | **at** *hh:mm* [*month day year*] [*text*] | **cancel**]

Parameter description

Parameter	Description
text	Cause to restart, 1-255 bytes
in *mmm hh:mm*	The system is restarted after specified time interval.
at *hh:mm month day year*	The system is restarted at the specified time. Up to 200 days is supported
month	Month in the range January to December
day	Date in the range 1 to 31
year	Year in the range 1993 to 2035

	cancel	Cancel scheduled restart.

Command mode	Privileged mode.
Usage guidelines	This command is used to restart the device at specified time, which may facilitate the management.

2.2.13 service config

This command is used to enable the device to first download the boot configuration file from a remote network server. The **no** form of this command is used to disable this function.

service config

no service config

Parameter description

Parameter	Description
-	-

Default configuration	Disabled.
Command mode	Global configuration mode.

Usage guidelines

This command needs to be used in combination with the boot config and boot network commands. When booting the device, the system loads the configuration file according to the following principles:

- If the service config command is not configured, the sequence of loading the configuration file is as follows: boot configuration filename configured using the boot config command, flash:/config.text, network boot configuration filename configured using the boot network command, and the default factory-delivered configuration (null configuration).
- If the service config command is configured, the sequence of loading the configuration file is as follows: network boot configuration filename configured using the boot network command, boot configuration filename configured using the boot config command, flash:/config.text, and the default factory-delivered configuration (null configuration).
- When loading the files in sequence, the system will not load the other configuration files as long as one configuration file is successfully loaded.

Caution

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

Examples

The example below enables the device to first download the boot configuration file from a remote network server and configure the network boot configuration filename:

```
DES-7200(config)# service config
DES-7200(config)# boot network tftp://192.168.7.24/config.text
```

Related commands

Command	Description
boot config	Set the boot configuration filename for the device.
boot network	Set the network boot configuration filename for the device.

2.2.14 session-timeout

To configure the session timeout for the remote terminal established in current LINE, use the **session-timeout** command.When the session timeout for the remote terminal in the LINE is cancelled, the session will never be timeout.

session-timeout *minutes* [**output**]

no session-timeout

Parameter description

Parameter	Description
minutes	The minutes of specified timeout.
output	Regard data output as the input to determine whether timeouts.

Default configuration

The default timeout is 0 min.

Command mode

LINE configuration mode.

Usage guidelines

If there is no input/output information for the session to the remote terminal established in current LINE within specified time, this connection will be interrupted, and this LINE will be restored to the free status.

Examples

The example below specifies the timeout of session is 5 minutes.

```
DES-7200(config-line)#exec-timeout 5 output
```

2.2.15 speed

To set speed at which the terminal transmits packets, execute the **speed** *speed* command in the line configuration mode. To restore the speed to its default value, run the **no speed** command.

speed *speed*

Parameter description

Parameter	Description
speed	Transmission rate (bps) on the terminal. For serial ports, the optional rates are 9600, 19200, 38400, 57600, and 115200 bps. The default rate is 9600 bps.

Command mode	Global configuration mode.
Default Configuration	The default rate is 9600.
Usage guidelines	This command sets the speed at which the terminal transmits packets.

Examples	The following example shows how to configure the rate of the serial port to 57600 bps:
	`DES-7200(config)#`
	`DES-7200(config)# line console 0`
	`DES-7200(config-line)# speed 57600`
	`DES-7200(config-line)#`

2.2.16 write

To perform the read/write operation for the device configurations (startup configuration or system configuration), execute the privileged user command **write**.

write [**memory | network | terminal**]

Parameter description

Parameter	Description
memory	Write the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**.
network	Save the system configuration into the TFTP server, which is equivalent to **copy running-config tftp**.
terminal	Show the system configuration, which is equivalent to **show running-config**.

Command mode	Privileged mode.

Usage guidelines

Despite of the alternative command, these commands have been widely used and accepted, so they are reserved to facilitate user's operation.

The **no** form with the command is equivalent to add the **memory** operation.

Examples

The example below saves the device configuration:

```
DES-7200# write
Building configuration...
[OK]
```

Related commands

Command	Description
show running-config	View the system configuration.
copy	Copy the device configuration files.

2.3 Showing Related Commands

2.3.1 show boot

Use this command to show the boot related configuration of the device.

show boot {config | network |system | ip}

	Parameter	Description
Parameter description	**config**	Show the configuration of the startup-config filename.
	network	Show the configuration of the network startup-config filename.
	system	Show the configuration of the startup main program filename.
	ip	Show the configuration of local IP address used in the device starting.

Command mode	Privileged mode

Usage guidelines

This command is used to show current boot related configuration of the device.

Note

The size and modified time of the files in the remote TFTP servers are shown as “N/A”. When perform the **show boot system** command, if the corresponding main program does not exist, the size and modified time of the file are also shown as “N/A”

Examples

1.The example below shows the configuration of the startup-config filename:

```
DES-7200# show boot config
Boot config file: [/config_main.text]
Service config: [Disabled]
```

2.The example below shows the configuration of network startup-config filename:

```
DES-7200# show boot network
Network config file: [tftp://192.168.7.24/config.text]
Service config: [Enabled]
```

3.The example below shows the configuration of the main program filename and boot priority:

```
DES-7200# show boot system
Boot system config:
================================================
Prio     Size            Modified  Name
---- --------- ------------------ -----------------
 1
 2
 3
 4
5     3205120 2008-08-26 05:22:46 flash:/firmware.bin
6
7
8     3205120 2008-08-26 05:25:09 flash:/firmware_bak.bin
9           N/A                  N/A
tftp://192.168.7.24/
                                   firmware.bin
10
================================================
```

4.The example below shows the configuration of local IP address that used in the device starting:

```
DES-7200# show boot ip
System boot ip: [192.168.7.11]
```

2.3.2 show mainfile

This command is used to show the current filename of the boot main program.

show mainfile

Parameter description

Parameter	Description
-	-

Command mode

Privileged mode

Usage guidelines

This command is used to show the current filename of the boot main program.

Examples	`DES-7200# show mainfile` `MainFile name: /firmware.bin`

Related commands

Command	Description
boot system	Set the filename of the boot main program.

2.3.3 show clock

To view the system time, execute the privileged user command **show clock**.

show clock

Parameter description

Parameter	Description
-	-

Command mode	Privileged mode
Usage guidelines	This command is used to view current system clock.

Examples	The example below is an execution result of the **show clock** command:
	`DES-7200# show clock`
	`clock: 2003-3-17 10:27:21`

Related commands

Command	Description
clock set	Set the system clock.

2.3.4 show line

To show the configuration of a line, execute the **show line** command in the privileged mode.

show line {**console** *line-num* | **vty** *line-num* **|** *line-num*}

Parameter description

Parameter	Description
console	Show the configuration of a console line.

	vty	Show the configuration of a vty line.
	line-num	Number of the line

Command mode	Privileged mode.
Usage guidelines	This command shows the configuration information of a line.

Examples	The following example shows the configuration of console port:
	`DES-7200# show line console 0`
	`CON Type speed Overruns`
	`* 0 CON 9600 45927`
	`Line 0, Location: "", Type: "vt100"`
	`Length: 24 lines, Width: 79 columns`
	`Special Chars: Escape Disconnect Activation`
	`^^x none ^M`
	`Timeouts: Idle EXEC Idle Session`
	`never never`
	`History is enabled, history size is 10.`
	`Total input: 53564 bytes`
	`Total output: 395756 bytes`
	`Data overflow: 27697 bytes`
	`stop rx interrupt: 0 times`

2.3.5 show reload

To show the restart settings of the system, execute the **show reload** command in the privileged EXEC mode.

show reload

Parameter description	N/A.
Command mode	Privileged mode.
Usage guidelines	Use this command to show the restart settings of the system.
Examples	The following example shows the restart settings of the system:

```
DES-7200# show reload
Reload scheduled in 595 seconds.
At 2003-12-29 11:37:42
Reload reason: test.
```

2.3.6 show running-config

To show the configuration information current device system is running, execute the privileged user command **show running-config**.

show running-config

Command mode	Privileged mode.

2.3.7 show startup-config

To view the configuration of device stored in the Non Volatile Random Access Memory (NVRAM), execute the privileged user command **show startup-config**.

show startup-config

Command mode	Privileged mode.
Usage guidelines	The configuration of device stored in the NVRAM is that executed when the device is startup.

2.3.8 show version

To view the information of the system, execute the command **show version** in the privileged mode.

show clock [**slots | devices| module**]

Parameter description

Parameter	Description
slots	Current slot information of the device.
module	Current module information of the device.
devices	Current device information

Command mode	Privileged mode
Usage guidelines	This command is used to view current system information, mainly including the system start time, version information, device information, serial number ,etc.

Examples	The example below shows the system information.
	`DES-7200# show clock detail`
	`clock: 2003-3-17 10:27:21`
	`Clock read from calendar when system boot.`
	`DES-7200# show version`
	`System description : DES-7200 Dual Stack Multi-Layer Switch By D-Link Corporation`
	`System start time: 1970-6-14 11:49:53`
	`System uptime: 3:17:1:17`
	`System hardware version: 2.0`
	`System software version: 10.3.00(4), Release(34679)`
	`System boot version: 10.2.34077`
	`System CTRL version: 10.2.24136`
	`System serial number: 1234942570001`

2.3.9 show web-server status

This command is used to show the configuration and status of a web server.

show web-server status

Parameter description	**Parameter**	**Description**
	-	-

Command mode	Privileged mode
Usage guidelines	N/A

Examples	The example below is an execution result of the **show web-server status** command:
	`DES-7200# show web-server status`
	`http server status : enabled`
	`http server port : 80`

```
https server status:  enabled
https server port: 443
```

3 SSH Configuration Commands

3.1 Related Configuration Commands

3.1.1 crypto key generate

In global configuration mode, use this command to generate a public key on the SSH server:

crypto key generate {**rsa|dsa**}

Parameter description

Parameter	Description
rsa	Generate an RSA key.
dsa	Generate a DSA key.

Default configuration

By default, the SSH server does not generate a public key.

Command mode

Global configuration mode.

Usage guidelines

When you need to enable the SSH Server service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

Caution

A key can be deleted by using the **crypto key zeroize** command. The **no crypto key generate** command is not available.

Examples	DES-7200# **configure terminal** DES-7200(config)# **crypto key generate rsa**

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.
crypto key zeroize {rsa | dsa}	Delete DSA and RSA keys and disable the SSH Server function.

3.1.2 crypto key zeroize

In global configuration mode, use this command to delete the public key on the SSH server.

crypto key zeroize {**rsa | dsa**}

Parameter description

Parameter	Description
rsa	Delete the RSA key.
dsa	Delete the DSA key.

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	This command deletes the public key of the SSH Server. After the key is deleted, the SSH Server state becomes DISABLE. If you want to disable the SSH Server, run the **no enable service ssh-server** command.
Examples	DES-7200# **configure terminal** DES-7200(config)# **crypto key zeroize** *rsa*

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.
crypto key generate {rsa|dsa}	Generate DSA and RSA keys.

3.1.3 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH Server. Use the **no** form of this command to restore it to the default setting.

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter description

Parameter	Description
retry times	Authentication retry times

Default configuration

The default authentication retry times are 3.

Command mode

Global configuration mode.

Usage guidelines

User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to view the configuration of the SSH Server.

Examples

The following example sets the authentication retry times to 2:

```
DES-7200# configure terminal
DES-7200(config)# ip ssh authentication-retries 2
```

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.

3.1.4 ip ssh time-out

Use this command to set the authentication timeout for the SSH Server. Use the **no** form of this command to restore it to the default setting.

ip ssh time-out *time*

no ip ssh time-out

Parameter description

Parameter	Description
time	Authentication timeout

Default configuration

The timeout value is 120s by default.

Command mode

Global configuration mode.

Usage guidelines

The authentication is considered timeout and failed if the authentication is not successful within 120s starting from receiving a connection request. Use the **show ip ssh** command to view the configuration of the SSH server.

Examples

The following example sets the timeout value as 100s:

```
DES-7200# configure terminal
DES-7200(config)# ip ssh time-out 100
```

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.

3.1.5 ip ssh version

Use this command to set the version of the SSH server. Use the **no** form of this command to restore it to the default setting.

ip ssh version {**1** | **2**}

no ip ssh version

Parameter description

Parameter	Description
1	Support the SSH1 client connection request.
2	Support the SSH2 client connection request.

Default configuration

SSH1 and SSH2 are compatible by default. When a version is set, the connection sent by the SSH client of this version is accepted only. The **no ip ssh version** command can also be used to restore it to the default setting.

Command mode

Global configuration mode.

Usage guidelines

This command is used to configure the SSH connection protocol version supported by SSH Server. By default, the SSH Server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH Server. Use the **show ip ssh** command to show the current status of SSH Server.

Examples

The following example sets the version of the SSH Server:

```
DES-7200# configure terminal
DES-7200(config)# ip ssh version 2
```

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.

3.2 Showing Related Commands

3.2.1 disconnect ssh

Use this command to disconnect the established SSH connection.

disconnect ssh [vty] *session-id*

Parameter description

Parameter	Description
session-id	ID of the established SSH connection session.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

Examples

```
DES-7200# disconnect ssh 1   Or
DES-7200# disconnect ssh vty 1
```

Related commands

Command	Description
show ssh	Show the information about the established SSH connection.
clear line vty *line_number*	Disconnect the current VTY connection.

3.2.2 show crypto key mypubkey

Use this command to show the information about the public key part of the public key on the SSH Server.

show crypto key mypubkey {rsa/dsa}

Parameter description

Parameter	Description
rsa	Show the public key part of the RSA key.
dsa	Show the public key part of the DSA key.

Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the information about the public key part of the generated public key on the SSH Server, including key generation time, key name, contents in the public key part, etc.
Examples	`DES-7200# show crypto key mypubkey rsa`

Related commands

Command	Description
crypto key generate {rsa | dsa}	Generate DSA and RSA keys.

3.2.3 show ip ssh

Use this command to show the information of the SSH Server.

show ip ssh

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the information of the SSH Server, including version, enablement state, authentication timeout, and authentication retry times. Note: If no key is generated for the SSH Server, the SSH version is still unavailable even if this SSH version has been configured.

Examples	`DES-7200# show ip ssh`

Related commands

Command	Description
ip ssh version {**1** | **2**}	Configure the version for the SSH Server.
ip ssh time-out time	Set the authentication timeout for the SSH Server.
ip ssh authentication-retries	Set the authentication retry times for the SSH Server.

3.2.4 show ssh

Use this command to show the information about the SSH connection.

show ssh

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the information about the established SSH connections, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.
Examples	`DES-7200# show ssh`
Related commands	N/A.

4 LINE Configuration Commands

4.1 Configuration Related Commands

4.1.1 access-class

Set the applied ACL (Access Control List) in Line. Use the **access-class** { *access-list-number* | *access-list-name* } **{ in | out }** command to configure the ACL in Line. Use the **no access-class** {*access-list-number* | *access-list-name*} **{in | out}** command to cancel the ACL configuration in LINE.

access-class { *access-list-number* | *access-list-name* } {**in | out**}

no access-class { *access-list-number* | *access-list-name* } {**in | out**}

Parameter description

Parameter	Description
access-list-number| *access-list-name*	Specify the ACL defined by access-list
in	Perform access control over the incoming connections
out	Perform access control over the outgoing connections

Default configuration

By default, no ACL is configured under Line. All connections are accepted, and all outgoing connections are allowed.

Command mode

Line configuration mode.

Usage guidelines

This command is used to configure ACLs under Line. By default, all the incoming and outgoing connections are allowed, and no connection is filtered. After **access-class** is configured, only the connections that pass access list

filtering can be established successfully. Use the **show running** command to view configuration information under Line.

Examples

In line vty 0 4, configure access-list for the accepted connections to 10:

```
DES-7200# configure terminal
DES-7200(config)# line vty 0 4
DES-7200(config-line)# access-class 10 in
```

Related commands

Command	Description
show running	Show status information

4.1.2 line

To enter the specified LINE mode, use the following command:

line [**console | vty**] *first-line* [*last-line*]

Parameter description

Parameter	Description
console	Console port
vty	Virtual terminal line, applicable for telnet/ssh connection.
first-line	Number of first-line to enter
last-line	Number of last-line to enter

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

Access to the specified LINE mode.

Examples

Enter the LINE mode from LINE VTY 1 to 3:

```
DES-7200(config)# line vty 1 3
```

Related

N/A.

commands	

4.1.3 line vty

This command can be used to increase the number of VTY connections currently available. The number of currently available VTY connections can be decreased by using the **no** form of this command.

line vty *line-number*

no line vty *line-number*

Default configuration	By default, there are five available VTY connections, numbered 0--4.
Command mode	Global configuration mode.
Usage guidelines	When you need to increase or decrease the number of available VTY connections, use the above commands.

Examples	Increase the number of available VTY connections to 20. The available VTY connections are numbered 0--19.
	`DES-7200(config)# line vty 19`
	Decrease the number of available VTY connections to 10. The available VTY connections are numbered 0-9.
	`DES-7200(config)# line vty 10`

Related commands	N/A.

4.1.4 transport input

To set the specified protocol under Line that can be used for communication, use the **transport input** command. Use **default transport input** to restore the protocols under Line that can be used for communication to the default value.

transport input {all | ssh | telnet | none}

default transport input

Parameter description

Parameter	Description
all	Allow all the protocols under Line to be used for communication
ssh	Allow only the SSH protocol under Line to be used for communication
telnet	Allow only the Telnet protocol under Line to be used for communication
none	Allow none of protocols under Line to be used for communication

Default configuration

By default, VTY allows all the protocols to be used for communication. The default value of other types of TTYs is NONE, indicating that no protocols are allowed for communication. After some protocols are set to be available for communication, use the **default transport input** command to restore the setting to the default value.

Command mode

Line configuration mode.

Usage guidelines

This command is used to set the protocols in the Line mode that are available for communication. By default, VTY allows all the protocols for communication. After protocols available for communication are set, only these protocols can connect on the specific VTY successfully. Use the **show running** command to view configuration information under Line.

Note: You can restore the default configuration by using the **default transport input** command. The **no transport input** command is used to disable all the communication protocols in the LINE mode. The setting result is the same as that of **transport input none**.

Examples

Specify that only the Telnet protocol is allowed to login in line vty 0 4:

```
DES-7200# configure terminal
DES-7200(config)# line vty 0 4
DES-7200(config-line)# transport input telnet
```

Related commands	**Command**	**Description**
	show running	Show status information

5 Network Connectivity Test Tool Configuration Commands

5.1 Configuration Related Commands

5.1.1 ping

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

ping [vrf *vrf-name* | ip] [*ip-address* [length *length*] [ntimes *times*] [timeout *seconds*] [data *data*] [source *source*] [df-bit] [validate]]

Parameter description

Parameter	Description
vrf-name	VRF name
ip-address	Specifies an IPv4 address.
length	Specifies the length of the packet to be sent.
times	Specifies the number of packets to be sent.
seconds	Specifies the timeout time.
data	Specifies the data to fill in.
seconds	Specifies the source IPv4 address or the source interface. The loopback interface address(for example: 127.0.0.1) is not allowed to be the source address.
df-bit	Sets the DF bit for the IP address. DF bit=1 indicates not to segmentate the datagrams. By default, the DF bit is 0.
validate	Sets whether to validate the reply packets or not.

Default

Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

Command mode	Privileged mode.
Usage guidelines	The ping command can be used in the ordinary user mode and the privileged mode. In the ordinary mode, only the basic functions of ping are available. In the privileged mode, in addition to the basic functions, the extension functions of the ping are also available. For the ordinary functions of ping, five packets of 100Byte in length are sent to the specified IP address within the specified period (2s by default). If response is received, '!' is displayed. If no response is received, '.' displayed, and the statistics is displayed at the end. For the extension functions of ping, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Examples

The example below shows the ordinary ping.

```
DES-7200# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout
is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 1/2/10 ms
```

The example below shows the extension ping.

```
DES-7200# ping 192.168.5.197 length 1500 ntimes 100
timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.5.197,
timeout is 3 seconds, data ffff source 192.168.4.10:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip
min/avg/max = 2/2/3 ms
DES-7200#
```

Platform description	The command is supported by all equipments.

5.1.2 ping ipv6

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

ping [ipv6] [*ipv6-address* [length *length*] [ntimes *times*] [timeout *seconds*] [data *data*] [source *source*]

Parameter description

Parameter	Description
Ipv6-address	Specifies an IPv6 address.
length	Specifies the length of the packet to be sent.
times	Specifies the number of packets to be sent.
seconds	Specifies the timeout time.
data	Specifies the data to fill in.
source	Specifies the source IPv6 address or the source interface. The loopback interface address(for example: 127.0.0.1) is not allowed to be the source address.

Default

Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

Command mode

Privileged mode.

Usage guidelines

The ping ipv6 command can be used in the ordinary user mode and the privileged mode. In the ordinary mode, only the basic functions of ping ipv6 are available. In the privileged mode, in addition to the basic functions, the extension functions of the ping ipv6 are also available. For the ordinary functions of ping ipv6, five packets of 100Byte in length are sent to the specified IP address within the specified period (2s by default). If response is received, '!' is displayed. If no response is received, '.' displayed, and the statistics is displayed at the end. For the extension functions of ping ipv6, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Examples

The example below shows the ordinary ping ipv6.

```
DES-7200# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, timeout is
2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 1/2/10 ms
```

The example below shows the extension ping ipv6.

```
DES-7200# ping  ipv6 2000::1  length 1500 ntimes 100
timeout 3 data ffff source 192.168.4.10:
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout
is 3 seconds
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip
min/avg/max = 2/2/3 ms
```

Platform description

The command is supported by all ipv6 equipments.

5.1.3 traceroute

Execute the traceroute command to show all gateways passed by the test packets from the source address to the destination address.

traceroute [**vrf** *vrf-name* | **ip**] [*ip-address* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

Parameter description

Parameter	Description
vrf-name	VRF name
ip-address	Specifies an IPv4 address.
number	Specifies the number of probe packets to be sent.
source	Specifies the source IPv4 address or the source interface. The loopback interface address(for example: 127.0.0.1) is not allowed to be the source address.
seconds	Specifies the timeout time.
minimum maximum	Specifies the minimum and maximum TTL values.

Command mode

Privileged mode.

Usage guidelines

Use the **traceroute** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

Examples

The following is two examples of the application bout traceroute, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
DES-7200# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36

1     192.168.12.1        0 msec   0 msec   0 msec
2     192.168.9.2         4 msec   4 msec   4 msec
3     192.168.9.1         8 msec   8 msec   4 msec
4      192.168.0.10       4 msec   28 msec  12 msec
5      192.168.9.2        4 msec   4 msec   4 msec
6      202.101.143.154    12 msec  8 msec   24 msec
7      61.154.22.36       12 msec  8 msec   22 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
DES-7200# traceroute 202.108.37.42
  < press Ctrl+C to break >
Tracing the route to 202.108.37.42

1     192.168.12.1      0 msec    0 msec  0 msec
2     192.168.9.2       0 msec    4 msec  4 msec
3     192.168.110.1     16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129      12 msec   28 msec  12 msec
6     61.154.8.17       8 msec    12 msec  16 msec
7     61.154.8.250      12 msec   12 msec  12 msec
8     218.85.157.222    12 msec   12 msec  12 msec
9      218.85.157.130   16 msec   16 msec  16 msec
10     218.85.157.77    16 msec   48 msec  16 msec
11     202.97.40.65     76 msec   24 msec  24 msec
12     202.97.37.65     32 msec   24 msec  24 msec
13     202.97.38.162    52 msec   52 msec  224 msec
14     202.96.12.38     84 msec   52 msec  52 msec
15     202.106.192.226  88 msec   52 msec  52 msec
16     202.106.192.174    52 msec   52 msec  88 msec
17     210.74.176.158   100 msec  52 msec  84 msec
18     202.108.37.42    48 msec   48 msec  52 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent time are displayed, and gateway 4 fails.

```
DES-7200# traceroute www.ietf.org

Translating "www.ietf.org"...[OK]
  < press Ctrl+C to break >
Tracing the route to 64.170.98.32

 1     192.168.217.1     0 msec  0 msec  0 msec
 2     10.10.25.1        0 msec  0 msec  0 msec
 3     10.10.24.1        0 msec  0 msec  0 msec
 4     10.10.30.1        10 msec 0 msec  0 msec
 5     218.5.3.254       0 msec  0 msec  0 msec
 6     61.154.8.49       10 msec 0 msec  0 msec
 7     202.109.204.210   0 msec  0 msec  0 msec
 8     202.97.41.69      20 msec 10 msec 20 msec
 9     202.97.34.65      40 msec 40 msec 50 msec
10     202.97.57.222     50 msec 40 msec 40 msec
11     219.141.130.122   40 msec 50 msec 40 msec
```

```
12    219.142.11.10     40 msec 50 msec 30 msec
13    211.157.37.14     50 msec 40 msec 50 msec
14    222.35.65.1       40 msec 50 msec 40 msec
15    222.35.65.18      40 msec 40 msec 40 msec
16    222.35.15.109     50 msec 50 msec 50 msec
17    *      *      *
18    64.170.98.32   40 msec 40 msec 40 msec
```

Platform description	The command is supported by all equipments.

5.1.4 traceroute ipv6

Use this command to show all gateways passed by the test packets from the source address to the destination address.

traceroute [**ipv6**] [*ip-address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

Parameter description

Parameter	Description
Ipv6-address	Specifies an IPv6 address.
number	Specifies the number of probe packets to be sent.
seconds	Specifies the timeout time.
minimum maximum	Specifies the minimum and maximum TTL values.

Command mode	Privileged mode.
Usage guidelines	Use the **traceroute ipv6** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.
Examples	The following is two examples of the application bout traceroute ipv6, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully. 1. When the network is connected smoothly:

```
DES-7200# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1        0 msec  0 msec  0 msec
2     3001::1        4 msec  4 msec 4 msec
3     3002::1        8 msec  8 msec  4 msec
4     3004::1        4 msec  28 msec  12 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~4) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
DES-7200# traceroute ipv6 3004::1
 < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1        0 msec  0 msec  0 msec
2     3001::1        4 msec  4 msec 4 msec
3     3002::1        8 msec  8 msec  4 msec
4     * * *
5     3004::1        4 msec  28 msec  12 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~5) and the spent time are displayed, and gateway 4 fails.

DES-7200

Ethernet Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 Interface Configuration Commands

1.1 Configuration Related Commands

1.1.1 carrier-delay

In the interface configuration mode, execute the **carrier-delay** command to set the carrier delay on the interface, and the **no carrier-delay** command to restore it to the default value.

carrier-delay [*seconds*]

no carrier-delay

Parameter description	**Parameter**	**Description**
	seconds	Optional parameter in the range of 1 to 60 seconds

Default configuration	The default carrier delay is 2 seconds.
Command mode	Interface configuration mode

Usage guidelines	This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation. If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.

Examples	The following example shows how to configure the carrier delay of serial interface to 5 seconds:
	`DES-7200(config)# interface gigabitethernet 1/1`
	`DES-7200(config)# carrier-delay 5`

1.1.2 clear counters

Use this command to clear the counters on the specified interface.

clear counters [*interface-id*]

Parameter description

Parameter	Description
interface-id	Interface type and interface ID

Command mode

Privileged mode.

Usage guidelines

In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

Examples

```
DES-7200# clear counters gigabitethernet 1/1
```

Related commands

Command	Description
show interfaces	Show the interface information.

1.1.3 clear interface

Reset the interface hardware.

clear interface *interface-id*

Parameter description

Parameter	Description
interface-id	Interface type and interface ID

Command mode

Privileged mode.

Usage guidelines

This command is only used on the switch port, member port of the L2 Aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

Examples

```
DES-7200# clear interface gigabitethernet 1/1
```

Related commands

Command	Description
shutdown	Shutdown the interface.

1.1.4 description

Use this command to set the alias of interface.. Use the **no** form of the command to restore the default setting.

description *string*

no description

Parameter description

Parameter	Description
string	Interface alias

Default configuration

By default, there is no alias.

Command mode

Interface configuration mode.

Usage guidelines	Use **show interfaces** to display the interface information, including the alias.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# description GBIC-1
```

Related commands

Command	Description
show interfaces	Show the interface information.

1.1.5 duplex

Use the **duplex** command in the interface configuration mode to specify the duplex mode for the interface. Use the **no** form of the command to restore it to the default setting.

duplex {**auto | full | half**}

no duplex

Parameter description

Parameter	Description
auto	Self-adaptive full duplex and half duplex
full	Full duplex
half	Half duplex

Default configuration	Auto.
Command mode	Interface configuration mode.
Usage guidelines	The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

Examples

```
DES-7200(config-if)# duplex full
```

Related commands

Command	Description
show interfaces	Show the interface information.

1.1.6 flowcontrol

Use this command to enable or disable the flow control. Use the **no** form of the command to restore it to the default setting.

flowcontrol {**auto | off | on | receive {auto | off | on } | send {auto | off | on}**}

no flowcontrol

Parameter description

Parameter	Description
auto	Self-negotiate the flow control.
off	Disable the flow control.
on	Enable the flow control.
receive	Receiving direction of the non-symmetric flow control.
send	Sending direction of the non-symmetric flow control.

Default configuration

By default, flow control is disabled.

Command mode

Interface configuration mode.

Usage guidelines

Use **show interfaces** to display the flow control configurations.

Examples

This example shows how to enable flow control on fastEthernet port 1/1:

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# flowcontrol on
```

Related commands

Command	Description
show interfaces	Show the interface information.

1.1.7 interface aggregateport

Use this command to access or create an aggregate port and enter interface configuration mode. Use the **no** form of the command to remove this port.

interface aggregateport *port-number*

Parameter description

Parameter	Description
port-number	Aggregate port number. Its range depends on the equipment and extended modules.

Command mode

Global configuration mode.

Usage guidelines

According to some rules, you can add other ports to an aggregate port. All the port members of an aggregate port are considered in a whole, and their attributes depend on the ones of the aggregate port. You can use **show interfaces** or **show interfaces aggregateport** commands to display the interface configuration.

Examples

```
DES-7200(config)#interface aggregateport 3
DES-7200(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description

DES-7200 series support up to 8 port members and create up to 128 AP globally.

1.1.8 interface fastEthernet

Use this command to select a Ethernet interface, and enter the interface configuration mode.

interface fastEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	The range depends on the device and the extended module.

Command mode

Global configuration mode.

Usage guidelines	The **no** form of the command is not available, and this interface type cannot be deleted. Use **show interfaces** or **show interfaces fastEthernet** to display the interface configurations.
Examples	`DES-7200(config)# interface fastEthernet 1/2` `DES-7200(config-if)#`

Related commands

Command	Description
show interfaces	Show the interface information.

Platform Description	N/A

1.1.9 interface giagbitEthernet

Use this command to select a Gigabit Ethernet interface, and enter the interface configuration mode.

interface gigabitEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	The range depends on the device and the extended module.

Command mode	Global configuration mode.
Usage guidelines	The **no** form of the command is not available, and this interface type cannot be deleted. Use **show interfaces** or **show interfaces gigabitEthernet** to display the interface configurations.
Examples	`DES-7200(config)# interface gigabitEthernet 1/2` `DES-7200(config-if)#`

Related commands

Command	Description
show interfaces	Show the interface information.

1.1.10 interface tenGiagbitEthernet

Use this command to select a 10G Ethernet interface, and enter the interface configuration mode.

interface tenGigabitEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	The range depends on the device and the extended module.

Command mode

Global configuration mode.

Usage guidelines

The **no** form of the command is not available, and this interface type cannot be deleted. Use **show interfaces** or **show interfaces tenGigabitEthernet** to display the interface configurations.

Examples

```
DES-7200(config)# interface tenGigabitEthernet 1/2
DES-7200(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

Platform Description

No product supports this command till now.

1.1.11 interface vlan

Use the **interface vlan** command in the global configuration mode to access or create the SVI (Switch Virtual Interface). Use the **no** form of the command to remove the SVI.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Parameter description

Parameter	Description
vlan-id	VLAN ID. Its range depends by products.

Command mode	Global configuration mode.
Usage guidelines	Use **show interfaces** or **show interfaces vlan** to display the interface configurations.
Examples	`DES-7200(config)# interface vlan 2` `DES-7200(config-if)#`

Related commands

Command	Description
show interfaces	Show the interface information.

Platform Description	DES-7200 series devices support up to 2K SVI ports and 2K IP addresses.

1.1.12 line-detect

Use this command to detect the cable connection status.

line-detect

Command mode	Interface configuration mode.
Usage guidelines	This command is used to detect the line status and locate the problem in case of a line failure, for example, the line is torn down.

Examples

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#line-detect

Interface : GigabitEthernet 0/1
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state     length(meters)
---- ---------- --------------
A    Ok        1
pair state     length(meters)
---- ---------- --------------
```

```
B    Ok        2
pair state     length(meters)
---- ---------- --------------
C    Short     1
pair state     length(meters)
---- ---------- --------------
D    Short     1
```

Field	Description
pairs	Number of line pairs included. For example, the twisted pair includes four pairs of lines.
state	Status of the current line pair: OK, Short or Open. In general, the 100M twisted pairs A and B are OK, C and D are Short. The 1000M twisted pairs A, B, C and D are all OK.
length	Length of the line in meter. Only the length of the line pair whose status is OK takes effect. Since the length is calculated based on the transmission time of signal, there may have a certain difference. The length of the line pair whose status is Short or Open is the length from the port to the faulty point.

1.1.13 medium-type

Use this command to select the medium type for an interface. Use the **no** form of the command to restore it to the default setting.

medium-type { **auto-select [prefer [fiber | copper]] | fiber | copper** }

no medium-type

Parameter description

Parameter	Description
fiber	Optical interface.
prefer[fiber| copper]	The preferred medium type for the interface is selected.
auto-select	Auto-select the medium type for the interface.
copper	Copper interface.

Default configuration	Copper interface.
Command mode	Interface configuration (physical interface, except for AP and SVI)
Usage guidelines	If a port can be selected as an optical port or electrical port, you can only select one of them. Once the media type is selected, the attributes of the port, for example, status, duplex, flow control, and rate, all mean those of the currently selected media type. After the port type is changed, the attributes of the new port type take the default values, which can be modified as needed.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# medium-type copeer`

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description	The 12 SFP interfaces of the 24SFP/12GT line cards and 1210/100/1000M BASE-T interfaces allow for dynamic switching. The combo interface is not supported to automatically determine whether the current port is the SFP interface or the 10/100/1000M BASE-T interface.

1.1.14 mtu

Use this command to set the MTU supported on the interface.

mtu *num*

Parameter description

Parameter	Description
num	64 to 9216 (or 65536, which varies by products)

Default configuration	By default, the num is 1500.

Command mode	Interface configuration mode.
Usage guidelines	Set the maximum transmission unit (MTU) supported on the interface. DES-7200 series now supports the setting on physical interfaces.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# mtu 9216`

Related commands

Command	Description
show interfaces	Show the interface information.

1.1.15 shutdown

Use the **shutdown** command in the interface configuration mode to disable an interface. Use the **no** form of the command to enable a disabled port.

shutdown

no shutdown

Command mode	Interface configuration mode
Usage guidelines	Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

Examples	Shut down Ap 1**:**
	`DES-7200(config)# interface aggregateport 1`
	`DES-7200(config-if)# shutdown`
	Enable Ap 1**:**
	`DES-7200(config)# interface aggregateport 1`
	`DES-7200(config-if)# no shutdown`

Related commands

Command	Description
clear interface	Reset the hardware.

show interfaces	Show the interface information.

Note

If you use the script to run **no shutdown** frequently and rapidly, the system may prompt the interface status reversal.

1.1.16 snmp trap link-status

You can set whether to send LinkTrap on a port. If the function is enabled, the SNMP will send the LinkTrap when the link status of the port changes. The **no** form of this command prevents the SNMP from sending the LinkTrap.

snmp trap link-status

no snmp trap link-status

Default configuration

This function is enabled. If the link status of the port changes, the SNMP sends the LinkTrap.

Command mode

Interface configuration mode.

Usage guidelines

For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

Examples

Do not send LinkTrap on the interface:

```
DES-7200(config)# interface gigabitEthernet 1/1
DES-7200(config-if)# no snmp trap link-status
```

Following configuration shows how to configure the interface to forwarding Link trap:

```
DES-7200(config)# interface gigabitEthernet 1/1
DES-7200(config-if)# snmp trap link-status
```

Related commands

Command	Function
DES-7200(config-if)# **snmp trap link-status**	Enable sending LinkTrap on the interface.

	DES-7200(config-if)# **no snmp trap link-status**	Disable sending LinkTrap on the interface.

1.1.17 speed

Use this command to configure the speed on the port. Use the **no** form of the command to restore it to the default setting.

Parameter description

Parameter	Description
10	Means that the transmission rate of the interface is 10Mbps.
100	Means that the transmission rate of the interface is 100Mbps.
1000	Means that the transmission rate of the interface is 1000Mbps.
10G	Means that the transmission rate of the interface is 10Gbps.
auto	Self-adaptive

Default configuration

Auto.

Command mode

Interface configuration mode.

Usage guidelines

If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M or 100M.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# speed 100
```

Related commands

Command	Description
show interfaces	Show the interface information.

1.1.18 switchport

In the interface configuration mode, you can use **switchport** without any parameter to configure an interface as Layer 2 mode. Use the **no switchport** command without any parameter to configure it as Layer 3 interface.

switchport

no switchport

Default	All the interfaces are in Layer 2 mode by default.
Command mode	Interface configuration mode.
Usage guidelines	This command is valid only for physical interfaces. The **switchport** command is used to disable the interface and re-enable it. In this status, the device will send the information to indicate the connect status. If the interface is changed to Layer 3 mode from Layer 2, all the attributes in Layer 2 mode will be cleared.
Examples	`DES-7200(config-if)# switchport`

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description	DES-7200 series support the creation of L3 aggregate ports, up to 128 L3 Aps globally. Up to 2000 IP addresses are supported.

1.1.19 switchport access

Use this command to configure an interface as a statics access port and add it to a VLAN. Use the **no** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter description

Parameter	Description
vlan-id	The VLAN ID at which the port to be

		added.

Default configuration

By default, the switch port is an access port and the VLAN is VLAN 1.

Command mode

Interface configuration mode.

Usage guidelines

Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN.

If the port is a trunk port, the operation does not take effect.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# switchport access vlan 2
```

Related commands

Command	Description
switchport mode	Specify the interface as Layer 2 mode(switch port mode).
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

1.1.20 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the **no** form of the command to restore it to the default setting.

switchport mode {**access | trunk**}

no switchport mode

Parameter description

Parameter	Description
access	Configure the switch port as an access port.
trunk	Configure the switch port as a trunk port.

Default

The default mode of switch port is access port.

configuration	
Command mode	Interface configuration mode.
Usage guidelines	If a switch port mode is access port, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN. A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.
Examples	`DES-7200(config-if)# switchport mode trunk`

Related commands

Command	Description
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port.

1.1.21 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of the command to restore it to the default setting.

switchport trunk {**allowed vlan** {**all |** [**add | remove | except**] *vlan-list* }**| native vlan** *vlan-id*}

no switchport trunk {**allowed vlan | native vlan**}

Parameter description

Parameter	Description
allowed vlan *vlan-list*	Configure the list of VLANs allowed on the trunk port. *vlan-list* can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma (,), for example, 1 to 10, 20 to 25, 30, 33. all means that the allowed VLAN list contains all the supported VLANs; add means to add the specified VLAN list to the allowed VLAN list; remove means to remove the specified VLAN list from the allowed VLAN list; except means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
native vlan *vlan-id*	Specify the native VLAN.

Default configuration

The allowed VLAN list is all, the Native VLAN is VLAN1.

Command mode

Interface configuration mode.

Usage guidelines

Native VLAN:

A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged.

Allowed-VLAN List:

By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk by configuring allowed VLAN lists on a trunk.

Use **show interfaces switchport** to display configuration.

Examples

The example below removes port 1/15 from VLAN 2:

```
DES-7200(config)# interface fastethernet 1/15
DES-7200(config-if)# switchport trunk allowed vlan remove 2
DES-7200(config-if)# end
DES-7200# show interfaces fastethernet1/15 switchport
Switchport is enabled
Mode is trunk port
Access vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is
1,3-4094
```

Related commands

Command	Description
show interfaces	Show the interface information.
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.

1.2 Showing Related Command

1.2.1 show interfaces

Use this command to show the interface information and optical module information.

show interfaces [*interface-id*] [**counters | description | status | switchport | trunk | transceiver** [**alarm | diagnosis| line-detect**]]

Parameter description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
counters	The counters on the interface.
description	The description of the interface, including the link status.
status	All the link status of the Layer 2 interface, including the rate and duplex.
switchport	Layer 2 interface information.
trunk	Trunk port, applicable for physical port and aggregate port.

transceiver	Basic optical module information.
alarm	Alarm information of the optical module. The “None” is displayed when no fault exists.
diagnosis	Diagnosis parameter value of the optical module.
line-detect	Line detecting status of the port.

Default configuration

Show all the information.

Command mode

Privileged mode.

Usage guidelines

Show the basic information if no parameter is specified.

Examples

The follow example shows the interface information when the Gi0/1 is Trunk port:

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
```

```
   admin speed is AUTO, oper speed is Unknown
flow receive control admin status is OFF,flow send control
admin status is OFF,flow receive control oper status is
Unknown,flow send control oper status is Unknown
    broadcast Storm Control is OFF,multicast Storm
Control is OFF,unicast Storm Control is OFF
 Port-type: trunk
   Native vlan:1
   Allowed vlan lists:1-4094
   Active vlan lists:1, 3-4
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
     0 output errors, 0 collisions, 0 interface resets
```

The following example shows the interface information when the Gi0/1 is Access port:

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
```

```
   flow receive control admin status is OFF,flow send
control admin status is OFF,flow receive control oper
status is Unknown,flow send control oper status is Unknown
    broadcast Storm Control is OFF,multicast Storm
Control is OFF,unicast Storm Control is OFF
  Port-type: access
    Vlan id : 2
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

The following example shows the layer-2 interface information when the Gi0/1 is Hybrid port.

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow receive control admin status is OFF,flow send control admin
status is OFF,flow receive control oper status is Unknown,flow send
control oper status is Unknown
```

```
    broadcast Storm Control is OFF,multicast Storm
Control is OFF,unicast Storm Control is OFF
  Port-type: hybrid
    Tagged vlan id:2
    Untagged vlan id:none
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runs, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

The following example shows the layer-2 information of the Gi0/1.

```
DES-7200# show interfacesgigabitEthernet 0/1 switchport
Interface Switchport ModeAccess Native Protected VLAN
lists
--------- ---------- --------- ------ ------ ---------
GigabitEthernet 0/1 enabled Access 11  Disabled  ALL
```

Related commands

Command	Description
duplex	Duplex
flowcontrol	Flow control status.
interface gigabitEthernet	Select the interface and enter the interface configuration mode.
interface aggregateport	Create or access the aggregate port, and enter the interface configuration mode.
interface vlan	Create or access the switch virtual interface (SVI), and enter the interface configuration mode.
shutdown	Disable the interface.
speed	Configure the speed on the port.
switchport priority	Configure the default 802.1q interface priority.
switchport protected	Specify the interface as a protected port.

Caution

The functions of showing the optical module information, alarming the fault and diagnosing the parameters shall be used combining with the optical module of the D-Link.

To show the optical module and alarm the fault and diagnose the parameters, the function of Digital Diagnostic Monitoring must be supported by the optical module.

2 MAC Address Configuration Commands

2.1 Configuration Related Commands

2.1.1 address-bind

Use this command to configure IP address-MAC address binding.

address-bind *ip-address mac-address*

no address-bind *ip-address*

Parameter description

Parameter	Description
ip-address	IP address to be bound
mac-address	MAC address to be bound

Command mode

Global configuration mode.

Usage guidelines

If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

Examples

This is an example of binding the IP address 3.3.3.3 and the MAC address 00d0.f811.1112.

```
DES-7200(config)# address-bind 3.3.3.3 00d0.f811.1112
```

Related commands

Command	Description
show address-bind	Show the IP address-MAC address binding table.

Platform description

DES-7200 series support up to 1000 IP address-MAC address binding.

2.1.2 address-bind *ip-address*

Use this command to configure IP address-MAC address binding.

address-bind *ip-address mac-address*

no address-bind *ip-address*

Parameter description

Parameter	Description
ip-address	IP address to be bound
mac-address	MAC address to be bound

Command mode

Global configuration mode.

Usage guidelines

If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

Examples

This is an example of binding the IP address 3.3.3.3 and MAC address 00d0.f811.1112.

```
DES-7200(config)# address-bind 3.3.3.3 00d0.f811.1112
```

Related commands

Command	Function
show address-bind	Show the IP address-MAC address binding table.

Platform description

DES-7200 series support up to 1000 IP address-MAC address binding.

2.1.3 address-bind ipv6-mode

Use this command to set the IP mode of IP address binding.

Set the compatbile mode:

address-bind ipv6-mode compatible

Set the loose mode:

address-bind ipv6-mode loose

Set the compatbile mode:

address-bind ipv6-mode strict

Parameter description	N/A.
Command mode	Global configuration mode.
Default value	Strict mode
Usage guidelines	There are three IP address binding modes: compatible, loose and strict. The following table shows the forwarding rules corresponding to binding modes.

Mode	IPv4 forwarding rule	IPv6 forwarding rule
Strict	Only the packets matching IPv4 and MAC are forwarded.	No IPv6 packets are forwarded (default).
Loose	Only the packets matching IPv4 and MAC are forwarded.	All IPv6 packets are forwarded.
compatible	Only the packets matching IPv4 and MAC are forwarded.	Only the IPv6 packets whose source MAC address is the bound MAC address are forwarded.

Examples

Bind the IP address 192.168.5.2 and the MAC address 00do.f822.33aa and forward the corresponding packets:

```
DES-7200# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#  address-bind  00d0.f822.33aa  ip 192.168.5.2
DES-7200(config)# address-bind ipv6-mode compatible
```

Related commands	**Command** / **Function** **show address-bind uplink** / Show the exceptional port of the address binding.
Platform description	N/A

2.1.4 address-bind install

Use this command to install or uninstall the exceptional port.

address-bind install

no address-bind install

Parameter description	N/A.
Command mode	Global configuration mode.
Usage guidelines	If you have installed the exceptional port, you can run this command to make installation policy take effect.

Examples	Install fa 0/1 port:
	`DES-7200(config)# address-bind uplink fa0/1`
	`DES-7200(config)# address-bind install`

Related commands	**Command** / **Function** **show address-bind uplink** / Show the exceptional port of the address binding.
Platform description	The version must be firmware v10.1 and later.

2.1.5 address-bind uplink

Use this command to configure IP address-MAC address binding.

address-bind uplink *intf-id*

no address-bind uplink *intf-id*

Parameter description

Parameter	Description
intf-id	Exceptional port

Command mode

Global configuration mode.

Usage guidelines

If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

Examples

Following example is to set the fa 0/1 port as an exceptional port for address binding.

```
DES-7200(config)#address-bind uplink fa0/1
```

Related commands

Command	Function
show address-bind uplink	Show the exceptional port of address binding.

Platform description

The version must be firmware v10.1 and later.

2.1.6 clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

clear mac-address-table dynamic [address *mac-addr*] **[interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
dynamic	Clear all the dynamic MAC addresses.
address *mac-addr*	Clear the specified dynamic MAC address.
interface *interface-id*	Clear all the dynamic MAC addresses of the specified interface.

	vlan *vlan-id*	Clear all the dynamic MAC addresses of the specified VLAN.

Command mode

Privileged mode.

Usage guidelines

Use **show mac-address-table dynamic** to display all the dynamic MAC addresses.

Examples

Clear all the dynamic MAC addresses:

```
DES-7200# clear mac-address-table dynamic
```

Related commands

Command	Description
show mac-address-table dynamic	Use this command to display dynamic MAC address.

2.1.7 clear mac-address-table filtering

Use this command to clear the filtering MAC address.

clear mac-address-table filtering [**address** *mac-addr*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
filtering	Clear all the filtering MAC addresses.
address *mac-addr*	Clear the specified filtering MAC address.
vlan *vlan-id*	Clear all the filtering MAC addresses of the specified VLAN.

Command mode

Privileged mode.

Usage guidelines

Use **show mac-address-table filtering** to display all the filtering MAC addresses.

Examples

Clear the filtering MAC address 00d0.f800.0c0c:

```
DES-7200# clear mac-address-table filtering address 00d0.f800.0c0c
```

Related commands

Command	Description
mac-address-table filtering	Configure the filtering MAC address.
show mac-address-table filtering	Show the filtering MAC address.

2.1.8 clear mac-address-table static

Use this command to clear the static MAC address.

clear mac-address-table static [address *mac-addr*] **[interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
static	Clear all the static MAC addresses.
address *mac-addr*	Clear the specified static MAC address.
interface *interface-id*	Clear all the static MAC addresses of the specified interface.
vlan *vlan-id*	Clear all the static MAC addresses of the specified VLAN.

Command mode

Privileged mode.

Usage guidelines

Use **show mac-address-table static** to display all the static MAC addresses.

Examples

The example below is to clear the static MAC address 00d0.f800.073c**:**

```
DES-7200# clear mac-address-table static address
00d0.f800.073c
```

Related commands

Command	Description
mac-address-table static	Configure the static MAC address.
show mac-address-table static	Show the static MAC address.

2.1.9 mac-address-learning

Use this command to enable / disable the MAC address learning on the interface.

mac-address-learning

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	The MAC address learning could not be disabled on the interface with the security function enabled. The interface with the MAC address learning function disabled could not be configured the security function.
Examples	The following example disables the MAC address learning. `DES-7200(config-if)# no mac-address-learning`

2.1.10 mac-address-table aging-time

Use this command to specify the aging time of the dynamic MAC address. Use the **no** form of the command to restore it to the default setting.

mac-address-table aging-time *seconds*

no mac-address-table aging-time

Parameter description

Parameter	Description
seconds	Aging time of the dynamic MAC address (in seconds). The time range depends on the switch.

Default configuration 300 seconds.

Command mode	Global configuration mode.
Usage guidelines	Use **show mac-address-table aging-time** to display configuration. Use **show mac-address-table dynamic** to display the dynamic MAC address table.
Examples	`DES-7200(config)# mac-address-table aging-time 150`

Related commands

Command	Description
show mac-address-table aging-time	Use this command to display the aging time of the dynamic MAC address.
show mac-address-table dynamic	Use this command to display dynamic MAC address.

2.1.11 mac-address-table filtering

Use this command to configure the filtering MAC address. Use the **no** form of the command to remove the filtering address.

mac-address-table filtering *mac-address* **vlan** *vlan-id* [source | destination]

no mac-address-table filtering *mac-address* **vlan** *vlan-id*

Parameter description

Parameter	Description
mac-address	Filtering Address
vlan *vlan-id*	VLAN ID. Its range depends on the switch.
source	Filter the frame according to the souce MAC address only.
destination	Filter the frame according to the destination MAC address only.

Default configuration	No filtering address is configured by default. When configuring this command without the **source** or **destination** specified, the frame received in the specified VLAN, which has the same source/destination MAC address with the specified MAC address, will be filtered.

Command mode	Global configuration mode.
Usage guidelines	The filtering MAC address shall not be a multicast address. Use **show mac-address-table filtering** to display the filtering MAC addresses.
Examples	`DES-7200(config)# mac-address-table filtering 00d0f8000000 vlan 1`

Related commands

Command	Description
clear mac-address-table filtering	Clear the filtering MAC address.
show mac-address-table filtering	Show the filtering MAC address.

2.1.12 mac-address-table notification

Use this command to enable the MAC address notification function. You can use The **no** form of the command to disable this function.

mac-address-table notification [**interval** *value* | **history-size** *value*]

no mac-address-table notification [**interval** | **history-size**]

Parameter description

Parameter	Description
interval *value*	Specify the interval of sending the MAC address trap message, 1 second by default.
history-size *value*	Specify the maximum number of the entries in the MAC address notification table, 50 entries by default.

Default configuration	By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.
Command mode	Global configuration mode.

Usage guidelines	The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the **snmp-server enable traps mac-notification** command to enable or disable the switch to send the MAC address trap message.

Examples	`DES-7200(config)# mac-address-table notification`
	`DES-7200(config)# mac-address-table notification interval 40`
	`DES-7200(config)# mac-address-table notification history-size 100`

Related commands

Command	Description
snmp-server enable traps	Set the method of handling the MAC address trap message..
show mac-address-table notification	Show the MAC address notification configuration and the MAC address trap notification table.
snmp trap mac-notification	Enable the MAC address trap notification function on the specified interface.

2.1.13 mac-address-table static

Use this command to configure a static MAC address. Use the **no** form of the command to remove a static MAC address.

mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the specified entry
vlan-id	VLAN ID of the specified entry.
interface-id	Interface (physical interface or aggregate port) that packets are forwarded to

Default	No static MAC address is configured by default.

configuration	
Command mode	Global configuration mode.
Usage guidelines	A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use **show mac-address-table static** to display the static MAC address. Use **clear mac-address-table static** to clear static MAC address.
Examples	When the packet destined to 00d0 f800 073c arrives at VLAN4, it will be forwarded to the specified port gigabitethernet 1/1: `DES-7200(config)# mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet 1/1`

Related commands

Command	Description
show mac-address-table static	Show the static MAC address.
clear mac-address-table static	Clear the static MAC address.

Platform description	For DES-7200 series, the global entry number in the MAC address table is 16000 and the global static MAC address number is 1000.

2.1.14 mac-manage-learning dispersive

Use this command to set the management and learning mode of the dynamic MAC address to the dispersive mode.

Parameter description	N/A.

Command mode	Global configuration mode.
Usage guidelines	After the management and learning mode of the dynamic MAC address is set to the dispersive mode, the device can learn more MAC addresses.
Examples	N/A.

Related commands

Command	Function
show mac-address-table mac-manage-learning	Show the MAC address management and learning mode.

2.1.15 mac-manage-learning uniform

Use this command to set the management and learning mode of the dynamic MAC address to the uniform mode.

Parameter description	N/A.
Command mode	Global configuration mode.
Usage guidelines	Setting the management and learning mode of the dynamic MAC address to the uniform mode can improve the L2 switching efficiency. After changing the MAC learning mode, you must save it and restart before the new mode takes effect.
Examples	N/A.

Related commands

Command	Function
show mac-address-table mac-manage-learning	Show the MAC management and learning mode.

Platform description	N/A

2.1.16 mac-manage-learning uniform learning-synchronization

Use this command to synchronize the dynamic MAC address in the whole device in the uniform mode.

[no] mac-manage-learning uniform learning-sychronization

Parameter description	N/A.
Command mode	Global configuration mode.
Usage guidelines	In the uniform mode, the synchronization of the dynamic MAC address in the whole device can further improve the L2 switching efficiency. You can use the **no** form of this command to cancel the synchronization.
Examples	N/A.

Related commands

Command	Function
show mac-address-table mac-manage-learning	Show the MAC address management and learning mode.

Platform description	N/A

2.1.17 snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. You can use The **no** form of the command to disable this function.

snmp trap mac-notification {**added** | **removed**}

no snmp trap mac-notification {**added** | **removed**}

Parameter description

Parameter	Description
added	Notify when a MAC address is added.
removed	Notify when a MAC address is removed

Default configuration Disabled.

Command mode Interface configuration mode.

Usage guidelines Use **show mac-address-table notification interface** to display configuration.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# snmp trap mac-notification added
```

Related commands

Command	Description
mac-address-table notification	Enable MAC address notification.
show mac-address-table notification	Show the MAC address notification configuration and the MAC address notification table.

2.2 Showing Related Command

2.2.1 show address-bind

Use this command to show IP address-MAC address binding.

show address-bind

Command mode Privileged mode.

Usage guidelines N/A.

Examples

```
DES-7200# show address-bind
IP Address     Binding MAC Addr
------------   -----------------
3.3.3.3        00d0.f811.1112
3.3.3.4        00d0.f811.1117
```

Related commands

Command	Description
address-bind	Enable IP address-MAC address binding.

2.2.2 show address-bind uplink

Use this command to show the exceptional port.

show address-bind uplink

Command mode Privileged mode.

Usage guidelines N/A.

Examples

```
DES-7200# show address-bind uplink
Ports        State
------------ ------
Fa0/1        Disabled
Fa0/2        Disabled
……
```

Related commands

Command	Description
address-bind uplink	Set the exceptional port.

2.2.3 show mac-address-learning

Use this command to show the MAC address learning.

show mac-address-learning

Command mode Privileged mode.

Examples The following example shows the MAC address learning

```
DES-7200# show mac-address-learning
```

2.2.4 show mac-address-table address

Use this command to show all types of MAC addresses (including dynamic address, static address and filtering address)

show mac-address-table [**address** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
address *mac-addr*	Specified MAC address.
interface *interface-id*	Interface ID
vlan *vlan-id*	VLAN ID

Command mode

Privileged mode.

Command mode

```
DES-7200# show mac-address-table address 00d0.f800.1001
Vlan       MAC Address         Type    Interface
----------  ------------------- --------
1          00d0.f800.1001      STATIC   Gi1/1
```

Related commands

Command	Description
show mac-address-table static	Show the static MAC address.
show mac-address-table filtering	Show the filtering MAC address.
show mac-address-table dynamic	Show the dynamic MAC address.
show mac-address-table interface	Show all types of MAC addresses of the specified interface
show mac-address-table vlan	Show all types of MAC addresses of the specified VLAN
show mac-address-table count	Show the address counts in the MAC address table.

	show mac-address-table static	Show the static MAC address.
	show mac-address-table filtering	Show the filtering MAC address.

2.2.5 show mac-address-table aging-time

Use this command to display the aging time of the dynamic MAC address.

show mac-address-table aging-time

Command mode	Privileged mode.

Examples

```
DES-7200# show mac-address-table aging-time
Aging time   : 300
```

Related commands

Command	Description
mac-address-table aging-time	Specify the aging time of the dynamic MAC address.

2.2.6 show mac-address-table count

Use this command to display the mac-address-table count.

show mac-address-table count

Command mode	Privileged mode.

Examples

```
DES-7200# show mac-address-table count
Dynamic Address Count  : 51
Static  Address Count  : 0
Filter  Address Count  : 0
Total Mac Addresses    : 51
Total Mac Address Space Available: 8139
```

Related commands

Command	Description
show mac-address-table static	Display the static address.

show mac-address-table filtering	Display the filtering address.
show mac-address-table dynamic	Display the dynamic address.
show mac-address-table address	Display all the address information of the specified address.
show mac-address-table interface	Display all the address information of the specified interface.
show mac-address-table vlan	Display all the address information of the specified vlan.

2.2.7 show mac-address-table dynamic

Use this command to show the dynamic MAC address.

show mac-address-table dynamic [**address** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN of the entry
interface-id	Interface that the packet is forwarded to. (It may be a physical port or an aggregate port)

Default configuration

All the MAC addresses are displayed by default.

Command mode

Privileged mode.

Examples

```
DES-7200# show mac-address-table dynamic
Vlan    MAC Address         Type    Interface
------------------------ -------- ------------------
1    0000.0000.0001      DYNAMIC  gigabitethernet 1/1
1    0001.960c.a740      DYNAMIC  gigabitethernet 1/1
1    0007.95c7.dff9      DYNAMIC  gigabitethernet 1/1
```

```
1    0007.95cf.eee0      DYNAMIC  gigabitethernet 1/1
1    0007.95cf.f41f      DYNAMIC  gigabitethernet 1/1
1    0009.b715.d400      DYNAMIC  gigabitethernet 1/1
1    0050.bade.63c4      DYNAMIC  gigabitethernet 1/1
```

Related commands

Command	Description
clear mac-address-table dynamic	Clear the dynamic MAC address.

2.2.8 show mac-address-table filtering

Use this command to show the filtering MAC address.

show mac-address-table filtering [**addr** *mac-addr*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry

Command mode

Privileged mode.

Examples

```
DES-7200# show mac-address-table filtering
Vlan       MAC Address       Type    Interface
-------  ----------------- ------- -----------
  1       0000.2222.2222     FILTER Not available
```

Related commands

Command	Description
clear mac-address-table filtering	Clear the filtering MAC address.
mac-address-table filtering	Configure the filtering MAC address.

2.2.9 show mac-address-table interface

Use this command to show all the MAC address information of the specified interface (including static and dynamic MAC address).

show mac-address-table interface [*interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
interface-id	Show the MAC address information of the specified Interface(physical interface or aggregate port).
vlan-id	Show the MAC address information of the VLAN.

Command mode

Privileged mode.

Examples

```
DES-7200# show mac-address-table interface
gigabitethernet 1/1
Vlan    MAC Address    Type     Interface
-----  -------------- -------- ----------------
1     00d0.f800.1001  STATIC   gigabitethernet 1/1
1     00d0.f800.1002  STATIC   gigabitethernet 1/1
1     00d0.f800.1003  STATIC   gigabitethernet 1/1
1     00d0.f800.1004  STATIC   gigabitethernet 1/1
```

Related commands

Command	Description
show mac-address-table static	Show the static MAC address.
show mac-address-table filtering	Show the filtering MAC address.
show mac-address-table dynamic	Show the dynamic MAC address.
show mac-address-table address	Show all types of MAC addresses.
show mac-address-table vlan	Show all types of MAC addresses of the specified VLAN.
show mac-address-table count	Show the address counts in the MAC address table.

2.2.10 show mac-address-table mac-manage-learning

Use this command to show the management and learning mode of the dynamic MAC address.

Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	`DES-7200# show mac-address-table mac-manage-learning`
	`######MAC manage-learning`
	`running mode: uniform`
	`configuration mode: uniform`
	`dynamic address learning-synchronization: off.`

Related commands

Command	Function
mac-manage-learning uniform	Set the management and learning mode of the dynamic MAC address to the uniform mode.
mac-manage-learning uniform learning-synchronization	Synchronize the dynamic MAC address in the whole device.
mac-manage-learning dispersive	Set the management and learning mode of the dynamic MAC address to the dispersive mode.

2.2.11 show mac-address-table notification

Use this command to show the MAC address notification configuration and the MAC address notification table.

show mac-address-table notification [**interface** [*interface-id*] **| history**]

Parameter description

Parameter	Description
interface *interface-id*	Interface ID. Show the MAC address notification configuration on the interface.
history	Show the MAC address

	notification history.

Default configuration	The MAC address notification configuration is shown by default.
Command mode	Privileged mode.

Examples

```
DES-7200# show mac-address-table notification interface
Interface        MAC Added Trap  MAC Removed Trap
---------         --------------      --------------
GigabitEthernet1/14   Disabled       Disabled
DES-7200# show mac-address-table notification
MAC Notification Feature: Disabled
Interval between Notification Traps: 1 secs
Maximum Number of entries configured in History Table:1
Current History Table Length: 0
DES-7200# show mac-address-table notification history
History Index: 0
MAC Changed Message:
Operation:ADD Vlan: 1 MAC Addr: 00f8.d012.3456
GigabitEthernet 3/1
```

Related commands

Command	Description
mac-address-table notification	Enable MAC address notification.
snmp trap mac-notification	Enable the MAC address trap notification function on the specified interface.

2.2.12 show mac-address-table static

Use this command to show the static MAC address.

show mac-address-table static [**addr** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry
interface-id	Interface of the entry (physical interface or aggregate port)

Command mode	Privileged mode.

Examples

Show only static MAC addresses

```
DES-7200# show mac-address-table static
Vlan       MAC Address        Type    Interface
----------  ------------------- -------- ---------
1    00d0.f800.1001    STATIC   gigabitethernet 1/1
1    00d0.f800.1002    STATIC   gigabitethernet 1/1
1    00d0.f800.1003    STATIC   gigabitethernet 1/1
```

Related commands

Command	Description
mac-address-table static	Configure the static MAC address.
clear mac-address-table static	Clear the static MAC address.

2.2.13 show mac-address-table vlan

Use this command to show all types of MAC addresses of the specified VLAN

show mac-address-table vlan [*vlan-id*]

Parameter description

Parameter	Description
vlan-id	VLAN ID of the entry

Command mode	Privileged mode.

Examples

```
DES-7200# show mac-address-table vlan 1
Vlan       MAC Address        Type    Interface
----------  ------------------- -------- ---------
1    00d0.f800.1001    STATIC   gigabitethernet 1/1
1    00d0.f800.1002    STATIC   gigabitethernet 1/1
1    00d0.f800.1003    STATIC   gigabitethernet 1/1
```

Related commands

Command	Description
show mac-address-table static	Show the static MAC address.

show mac-address-table filtering	Show the filtering MAC address.
show mac-address-table dynamic	Show the dynamic MAC address.
show mac-address-table address	Show all types of MAC addresses.
show mac-address-table interface	Show all types of MAC addresses of the specified interface.
show mac-address-table count	Show the address counts in the MAC address table.

3 Aggregate Port Configuration Commands

3.1 Configuration Related Commands

3.1.1 aggregateport load-balance

Specify a load-balance algorithm. Use the **no** command to return it to the default setting.

aggregateport load-balance {**dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst ip** }

no aggregateport load-balance

Parameter description

Parameter	Description
dst-mac	Traffic is distributed according to the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
src-mac	Traffic is distributed according to the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.

Src-dst-ip	Traffic is distributed according to the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
dst-ip	Traffic is distributed according to the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Traffic is distributed according to the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-mac	Traffic is distributed according to the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.

Default configuration

Traffic is distributed according to the destination and source MAC addresses of the incoming packets.

Command mode

Global configuration mode.

Usage guidelines	Use **show aggregateport** to display load-balance configuration.
Examples	`DES-7200(config)# aggregateport load-balance dst-mac`

Related commands

Command	Description
show aggregateport load-balance	Use this command to display aggregate port configurations.

Platform description	N/A

3.1.2 port-group

Use this command to assign a physical interface to be a member port of an aggregate port. Use the **no** form of the command to remove the membership from the aggregate port.

port-group *port-group-number*

no port-group

Parameter description

Parameter	Description
port-group-number	Number of the member group of an aggregate port, the interface number of the aggregate port

Default configuration	By default, the physical port does not belong to any aggregate port.
Command mode	Interface configuration mode.
Usage guidelines	All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.
Examples	This example shows how to specify the Ethernet interface 1/3 and 1/4 as members of AP 3: `DES-7200(config)# interface gigabitethernet 1/3`

```
DES-7200(config-if)# port-group 3
```

Platform description	DES-7200 series support up to 8 member ports and create up to 128 AP globally.

3.2 Showing Related Command

3.2.1 show aggregateport

Use this command to display the aggregate port configurations.

show aggregateport {[*aggregate-port-number*] **summary** | **load-balance**}

Parameter description

Parameter	Description
aggregate-port-number	Number of the aggregate port.
load-balance	Show the load-balance algorithm on the aggregate port.
summary	Show the summary of the aggregate port.

Command mode

Privileged mode.

Usage guidelines

If the aggregate port number is not specified, all the aggregate port information will be displayed.

Examples

```
DES-7200# show aggregateport 1 summary
AggregatePort  MaxPorts       SwitchPort Mode   Ports
-------------  --------       -------------   ------
Ag1              8             Enabled     ACCESS
```

Related commands

Command	Description
aggregateport load-balance	Configure a load-balance algorithm of AP.

4 LACP Configuration Commands

4.1 Configuration Related Commands

4.1.1 port-group mode

Use this command to enable LACP and specify the group ID and the aggregation mode. Use the **no** form of this command to disable the LACP.

port-group *key* **mode {active | passive}**

no port-group

Parameter description

Parameter	Description
key	Specify the group ID on the port to be aggregated. The key values vary with the aggregation group numbers supported for different products.
active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Default configuration By default, the LACP function is disabled on the interface.

Command mode Interface configuration mode.

Usage N/A

guidelines

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# port-group 1 mode active
```

Related commands

Command	Description
lacp port-priority	Set the LACP port priority.

4.1.2 lacp port-priority

Use this command to set the LACP port priority. Use the **no** form of this command to return to the default value.

lacp port-priority *port-priority*

no lacp port-priority

Parameter description

Parameter	Description
port-priority	The port priority, in the range of 0-65535.

Default configuration

By default, the port priority is 32768.

Command mode

Interface configuration mode.

Usage guidelines

When multiple ports are to be aggregated, the ports with high priorities take precedence and the port with the highest priority is selected as the master port. The port priority sequence is determined according to the wire quality.

The LACP cannot be enabled on the ports with the function of forbidding the member ports to add to or leave the AP enabled; and the function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP member ports. The AP with the function of forbidding the member ports to add to or leave cannot configured as the LACP AP, and function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP AP.

The SYSLOG will be displayed when the LACP fails to

leave the AP due to external function limitations, such as: %LACP-5-UNBUNDLE_FAIL: Interface FastEthernet 0/1 failed to leave the AggregatePort 1. In this case, please modify the configuration to cancel the related configuration of forbidding the member ports to leave the AP, otherwise the normal packets transmission on the AP will be influenced.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# lacp port-priority 4096
```

Related commands

Command	Description
port-group *key* **mode** {**active** | **passive**}	Enable the LACP on the port and specify the aggregation group ID and operation mode.

4.1.3 lacp system-priority

Use this command to set the LACP system priority. The **no** form of it restores it to the default.

lacp system-priority *system-priority*

no lacp system-priority

Parameter description

Parameter	Description
system-priority	The LACP system priority, in the range of 0-65535.

Default configuration

By default, the system priority is 32768.

Command mode

Global configuration mode.

Usage guidelines

LACP system priority consists of the Layer2 management MAC address and its priority value, where the MAC address is fixed but the priority value is configurable. If two

priorities are equal, then the smaller the MAC address is, the higher the priority is. All LACP groups on the switch share the system priority. Changing the system priority may influence the whole aggregation groups on the switch.

Examples

```
DES-7200(config)# lacp system-priority 4096
```

Related commands

Command	Description
port-group *key* **mode** {**active** | **passive**}	Enable the LACP on the port and specify the aggregation group ID and operation mode.
lacp port-priority	Set the LACP port priority.

4.2 Showing Related Command

4.2.1 show lacp summary

Use this command to show the LACP aggregation information.

show lacp summary [*key***]**

Parameter description

Parameter	Description
key	Specify the aggregation group id to show. If it is not specified, all aggregation group information is shown by default.

Command mode

Privileged mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show LACP summary
Flags:S - Device is sending Slow LACPDUs   F - Device is sending
fast LACPDUs.
A - Device is in active mode.   P - Device is in passive mode.
Aggregate port 3:
Local information:
```

```
                  LACP port      Oper    Port    Port
Port    Flags    State    Priority    Key    Number  State
-------------------------------------------------------------
---
Gi0/1     SA         bndl         4096          0x3      0x1
0x3d
Gi0/2     SA         bndl         4096          0x3      0x2
0x3d
Gi0/3     SA         bndl         4096          0x3      0x3
0x3d
Partner information:
                  LACP port        Oper    Port    Port
Port    Flags    Priority    Dev ID    Key    Number   State
-------------------------------------------------------------
--
Gi0/1    SA    61440    00d0.f800.0002   0x3    0x1    0x3d
Gi0/2    SA    61440    00d0.f800.0002   0x3    0x2    0x3d
Gi0/3    SA    61440    00d0.f800.0002   0x3    0x3    0x3d
```

Field	Description
Local information	Show the local LACP information.
Port	Show the system port ID.
Flags	Show the port state flag: “S” indicates that the LACP is stable and in the state of periodically sending the LACPPDU; “A” indicates that the port is in the active mode.
State	Show the port aggregation information: “bndl” indicates that the port is aggregated; “Down” represents the disconnection port state; “susp” indicates that the port is not aggregated.

LACP Port Priority	Show the LACP port priority.
Oper Key	Show the port operation key.
Port Number	Show the port number.
Port State	Show the flag bit for the LACP port state.
Partner infomation	Partly show the LACP information of the peer port.
Dev ID	Partly show the system MAC information of the peer device.

Related commands

Command	Description
port-group *key* **mode**	Enable the LACP on the port and specify the aggregation group ID and operation mode.

5 VLAN Configuration Commands

5.1 Configuration Related Commands

5.1.1 add

Use this command to add one or a group Access interface into current VLAN. Use the **no** form of the command to remove the Access interface.

add interface { *interface-id* | **range** *interface-range* }

no add interface { *interface-id* | **range** *interface-range* }

Parameter description

Parameter	Description
interface-id	Layer-2 Ethernet interface or layer-2 AP port.
range *interface-range*	Range of the Layer-2 Ethernet interface or layer-2 AP port.

Default configuration

All layer-2 Ethernet interfaces are in the VLAN1.

Command mode

VLAN configuration mode.

Usage guidelines

- This command is only valid for the access port.
- The configuration of this command is the same as specifying the VLAN to which interface belongs in the interface configuration mode (that is the **switchport access vlan** v*lan-id*). For the two commands of adding the interface to the VLAN, the command configured later will overwrite the one configured before and take effect.
- The configuration of adding the layer-2 AP into current VLAN through this command will only take effect for the layer-2 AP port, but not for the member port of the layer-2 AP port.

Examples

The following example adds the interface GigabitEthernet 0/10 into the VLAN20.

```
DES-7200# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
DES-7200# show interface GigabitEthernet 0/10 switchport
Interface  Switchport  Mode  Access  Native Protected
VLAN lists
---------- --------     -----  -----  ---- ----------
-------
GigabitEthernet 0/10 enabled  ACCESS  20   1   Disabled
ALL
```

The following example adds the interface range GigabitEthernet 0/1-10 into the VLAN200.

```
DES-7200# configure terminal
SwitchA(config)#vlan 200
SwitchA(config-vlan)#add interface range GigabitEthernet
0/1-10
DES-7200# show vlan
SwitchA#show vlan
VLAN Name       Status                    Ports
----      -------                          ------------
----------------------------
1        VLAN0001                                STATIC
                              Gi0/11,Gi0/12,Gi0/13,Gi0/1
                              4,Gi0/15,
                              Gi0/16,Gi0/17,Gi0/18,Gi0/1
                              9,Gi0/20,Gi0/21,    Gi0/22,
```

```
                                    Gi0/23, Gi0/24
200  VLAN0200  STATIC    Gi0/1,Gi0/2,Gi0/3,Gi0/4,Gi0/5,
                                    Gi0/6,Gi0/7,Gi0/8,Gi0
                                    /9,Gi0/10
```

The following example adds the AggregatePort10 into the VLAN20.

```
DES-7200# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface aggregateport 10
DES-7200# show interface aggregateport 10 switchport
Interface  Switchport   Mode  Access  Native Protected
VLAN lists
---------- --------      -----  -----  ---- ----------
-------
AggregatePort 10 enabled  ACCESS  20   1   Disabled  ALL
```

Related commands

Command	Description
show interface *interface-id* **switchport**	Show the layer-2 interfaces.

5.1.2 name

Use the command to specify the name of a VLAN. Use the **no** form of the command to restore it to the default setting.

name *vlan-name*

no name

Parameter description

Parameter	Description
vlan-name	VLAN name

Default configuration

The default name of a VLAN is the combination of “VLAN” and VLAN ID, for example, the default name of the VLAN 2 is “VLAN0002”.

Command mode

VLAN configuration Mode.

Usage

You can view the VLAN settings by using the **show vlan**

guidelines	command.

Examples

```
DES-7200(config)# vlan 10
DES-7200(config-vlan)# name vlan10
```

Related commands

Command	Description
show vlan	Show member ports of the VLAN.

5.1.3 switchport access

Use this command to configure an interface as a statics access port and assign it to a VLAN. Use the **no** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Default configuration	By default, the switch port is an access port and the VLAN is VLAN 1.
Command mode	Interface configuration mode.
Usage guidelines	Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN. If the port is a trunk port, the operation does not take effect.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# switchport access vlan 2
```

Related commands

Command	Description
switchport mode	Specify the interface as Layer 2 mode (switch port mode).

	switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

5.1.4 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the **no** form of the command to restore the default setting.

switchport mode {**access** | **trunk | hybrid | uplink | dot1q-tunnel**}

no switchport mode

Parameter description

Parameter	Description
access	Configure the switch port as an access port.
trunk	Configure the switch port as a trunk port.
hybrid	Configure the switch port as a hybrid port.
uplink	Configure the switch port as an uplink port.
dot1q-tunnel	Configure the switch port as a 802.1Q tunnel port.

Default configuration

By default, the switch port is an access port.

Command mode

Interface configuration mode.

Usage guidelines

If a switch port mode is access port, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN.

A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.

Examples

```
DES-7200(config-if)# switchport mode trunk
```

Related commands

Command	Description
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

5.1.5 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of the command to restore the default setting.

switchport trunk {**allowed vlan** { **all** | [**add** | **remove** | **except**] *vlan-list* }| **native vlan** *vlan-id*}

no switchport trunk {**allowed vlan** | **native vlan** }

Parameter description

Parameter	Description
allowed vlan *vlan-list*	Configure the list of VLANs allowed on the trunk port. *vlan-list* can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma (,), for example, 1 to 10, 20 to 25, 30, 33. **all** means that the allowed VLAN list contains all the supported VLANs; **add** means to add the specified VLAN list to the allowed VLAN list; **remove** means to remove the specified VLAN list from the allowed VLAN list; **except** means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
native vlan *vlan-id*	Specify the native VLAN.

Default configuration

The default allowed-VLAN list is all the VLANs, the default native VLAN is VLAN 1.

Command mode	Interface configuration mode.
Usage guidelines	**Native VLAN:** A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged. **Allowed-VLAN List:** By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk port by configuring allowed VLAN lists on a trunk port . Use **show interfaces switchport** to display configuration.

Examples	The example below removes port 1/15 from VLAN 2:
	`DES-7200(config)# interface fastethernet 1/15`
	`DES-7200(config-if)# switchport trunk allowed vlan remove 2`
	`DES-7200(config-if)# end`
	`DES-7200# show interfaces fastethernet1/15 switchport`
	`Interface Switchport Mode Access Native Protected VLAN lists`
	`--------- --------- --------- ---------`
	`FigabitEthernet 1/15 enabled TRUNK 1 1 Disabled 1,3-4094`

Related commands

Command	Description
show interfaces	Show the interface information.
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.

5.1.6 vlan

Use this command to enter the VLAN configuration mode. Use the **no** form of the command to remove the VLAN.

vlan vlan-id

no vlan *vlan-id*

Parameter description

Parameter	Description
vlan-id	VLAN ID Default VLAN (VLAN 1) cannot be removed.

Command mode

Global configuration mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or pressing **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7200(config)# vlan 1
DES-7200(config-vlan)#
```

Related commands

Command	Description
show vlan	Show member ports of the VLAN.

5.2 Showing Related Commands

5.2.1 show vlan

Show member ports of the VLAN.

show vlan [**id** *vlan-id*]

Parameter description

Parameter	Description
vlan-id	VLAN ID

Default configuration

Show all the information by default.

Command mode

Privileged mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or pressing **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7200# show vlan id 1
VLAN Name      Status    Ports
---------- ------------ ------------
1   VLAN0001        STATIC    Fa0/1, Fa0/2
```

Related commands

Command	Description
name	VLAN name.
switchport access	Add the interface to a VLAN.

6 Super-VLAN Configuration Commands

6.1 Configuring Related Commands

6.1.1 subvlan

Use this command to set the sub VLAN of this super VLAN or delete sub VLAN.

subvlan *vlan-id-list*

no subvlan *[vlan-id-list]*

Parameter description

Parameter	Description
vlan-id-list	Sub VLAN ID of the VLAN. Multiple VLANs are supported.

Command mode

VLAN configuration Mode.

Usage guidelines

Use **no subvlan** command to delete all sub VLANs of this super VLAN.

Examples

```
DES-7200(config)# vlan 3
DES-7200(config-vlan)# supervlan
DES-7200(config-vlan)# subvlan 5
DES-7200(config-vlan)# subvlan 7-19
```

Related commands

Command	Description
show supervlan	Show the super VLAN information.

6.1.2 subvlan-address-range

Use this command to set the IP address range of the sub VLAN.

subvlan-address-range *start-ip end-ip*

no subvlan-address-range

Parameter description

Parameter	Description
start-ip	The start IP address of this sub VLAN
end-ip	The end IP address of this sub VLAN

Command mode

VLAN configuration Mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or press **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7200(config)# vlan 3
DES-7200(config-vlan)# subvlan-address-range
192.168.3.10 192.168.3.100
```

Related commands

Command	Description
show supervlan	Show the super VLAN information.

6.1.3 supervlan

Use this command to set the VLAN as a super VLAN.

supervlan

no supervlan

Parameter description

N/A.

Command mode

VLAN configuration Mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or press **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7200(config)# vlan 3
DES-7200(config-vlan)# supervlan
```

Related commands

Command	Description
show supervlan	Show the super VLAN information.

Platform description N/A.

6.1.4 proxy-arp

Use this command to enable the ARP agent function of a VLAN.

proxy -arp

no proxy -arp

Parameter description N/A.

Command mode VLAN configuration Mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or press **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7200(config)# vlan 3
DES-7200(config-vlan)# proxy-arp
```

Related commands

Command	Description
show supervlan	Show the super VLAN information.

Platform description N/A.

6.2 Showing Related Command

6.2.1 show supervlan

Use this command to show the configuration of the super VLAN and its sub VLANs.

show supervlan

show supervlan id *vlan-id*

Parameter description

Parameter	Description
vlan-id	VLAN ID

Command mode

Privileged mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show supervlan
supervlan id  supervlan arp-agent  subvlan id  subvlan
arp-agent  subvlan ip range
-------    ----------  -------------
-----------------
3               ON         4              ON
                           5              ON
```

7 Protocol VLAN Configuration Commands

7.1 Configuration Related Commands

7.1.1 protocol-vlan ipv4 *addr* mask *addr* vlan *id*

Use this command to configure the IP address, subnet mask and VLAN classification.

Parameter description

Parameter	Description
addr	IP address in the x.x.x.x format.
id	VLAN ID, the maximal VLAN the product supports

Default configuration N/A.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# protocol-vlan ipv4 192.168.100.3 mask 255. 255.255.0 vlan 100
```

Related commands

Command	Description
show protocol-vlan ipv4	
no protocol-vlan ipv4 *addr* **mask** *addr*	
no protocol-vlan ipv4	

Platform description The software version must be firmware v10.1 and later.

7.1.2 protocol-vlan ipv4

Use this command to enable configuring the IP address, subnet mask and VLAN classification.

Parameter description

Parameter	Description
-	-

Default configuration N/A.

Command mode Interface configuration mode.

Examples

```
DES-7200(config-if)# protocol vlan ipv4
```

Related commands

Command	Description
no protocol-vlan ipv4	-

Platform description The software version must be firmware v10.1 and later.

7.1.3 protocol-vlan profile *num* frame-type *type* ether-type *type*

Use this command to configure message type and Ethernet type profile.

Parameter description

Parameter	Description
num	Profile indexes
type	Type of message and Ethernet

Default configuration N/A.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# protocol-vlan  profile 1 frame-type
ETHERII ether-type aarp
```

Related commands

Command	Description
show protocol-vlan profile	
show protocol-vlan profile *num*	
no protocol-vlan profile	
no protocol-vlan profile *num*	

Platform description The software version must be firmware v10.1 and later.

7.1.4 protocol-vlan profile *num* vlan *id*

Use this command to apply some profile to an interface.

Parameter description

Parameter	Description
num	Profile indexes
id	VLAN ID, the maximal VLAN the product supports.

Command mode Interface mode.

Examples

```
DES-7200(config-if)# protocol-vlan profile 1 vlan 101
```

Related commands

Command	Description
show protocol-vlan profile	
show protocol-vlan profile *num*	
no protocol-vlan profile	
no protocol-vlan profile *num*	

Platform description	The software version must be firmware v10.1 and later.

7.2 Showing Related Commands

7.2.1 show protocol-vlan

Show the configuration of protocol VLAN.

show protocol-vlan

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged mode.
Examples	`DES-7200# show protocol-vlan`
Platform description	The software version must be firmware v10.1 and later.

8 Private VLAN Configuration Commands

8.1 Configuration Related Commands

8.1.1 private-vlan *type*

Use this command to configure the VLAN as the private VLAN.

private-vlan {**community | isolated | primary**}

no private-vlan {**community | isolated | primary**}

Parameter description

Parameter	Description
community	Configure it as the community VLAN.
isolated	Configure it as the isolated VLAN.
primary	Configure it as the primary VLAN.
no	Delete the corresponding private VLAN configuration.

Default configuration

No private VLAN is configured.

Command mode

VLAN configuration Mode.

Examples

```
DES-7200(config)# vlan 22
DES-7200(config-vlan)# private-vlan primary
```

Related commands

Command	Description
show vlan private-vlan	

Platform description	The software version must be firmware v10.1 and later.

8.1.2 private-vlan association

Use this command to associate the secondary VLAN with the primary command.

private-vlan association {*svlist* **| add** *svlist* **| remove** *svlist*}

no private-vlan association

Parameter description

Parameter	Description
svlist	The secondary VLAN list
no	Remove the association between the primary VLAN and all the secondary VLANs.

Default configuration	No association.
Command mode	Primary VLAN configuration Mode.

Examples

```
DES-7200(config)# vlan 22
DES-7200(config-vlan)# private-vlan association add
24-26
```

Related commands

Command	Description
show vlan private-vlan	

Platform description	The software version must be firmware v10.1 and later.

8.1.3 private-vlan mapping

Use this command to map the secondary VLAN to the L3 SVI interface.

private-vlan mapping {*svlist* **| add** *svlist* **| remove** *svlist*}

no private-vlan mapping

Parameter description

Parameter	Description
svlist	secondary VLAN list
no	Delete the mapping.

Command mode

The interface mode corresponding to the primary VLAN

Examples

```
DES-7200(config)# interface vlan 22
DES-7200(config-if)# private-vlan mapping add 24-26
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be firmware v10.1 and later.

8.1.4 switchport mode private-vlan

Use this command to declare the private VLAN mode of the interface.

switchport mode private-vlan {**host | promiscuous** }

no switchport mode

Parameter description

Parameter	Description
host	Host mode of the private VLAN
promiscuous	Promiscuous mode of the private VLAN
no	Delete the private VLAN configuration of the port.

Command mode

Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitEthernet0/2
DES-7200(config-if)# switchport mode private-vlan host
```

Related

Command	Description

	show vlan private-vlan	

Platform description The software version must be firmware v10.1 and later.

8.1.5 switchport private-vlan host-association

Use this command to associate the primary VLAN, which is associated with the private VLAN mode of the interface, with the secondary VLAN.

switchport private-vlan host-association *p_vid s_vid*

no switchport private-vlan host-association

Parameter description

Parameter	Description
p_vid	Primary VID.
s_vid	Secondary VID
no	Delete the host port from the private VLAN.

Command mode Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode private-vlan host
DES-7200(config-if)# switchport private-vlan
host-association 22 23
```

Related commands

Command	Description
show vlan private-vlan	

Platform description The software version must be firmware v10.1 and later.

8.1.6 switchport private-vlan association trunk

Use this command to associate the trunk port in the private VLAN mode, which is associated with the primary VLAN and the secondary VLAN.

switchport private-vlan association trunk *p_vid s_vid*

no switchport private-vlan association trunk

Parameter description

Parameter	Description
p_vid	Primary VID.
s_vid	Secondary VID
no	Delete the host port from the private VLAN.

Command mode

Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# switchport private-vlan
association trunk 202 203
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be firmware v10.4 (3) and later.

8.1.7 switchport private-vlan mapping

Use this command to configure the promiscuous secondary VLANs that the promiscuous mode of the private VLAN maps.

switchport private-vlan mapping *p_vid* {*svlist*|**add** *svist* |**remove** *svlist*}

no switchport private-vlan mapping

Parameter description

Parameter	Description
p_vid	Primary VID
svlist	Secondary VLAN list.
no	Remove all the promiscuous secondary VLANs.

Default configuration

No promiscuous secondary VLAN is configured.

Command mode	Hybrid interface configuration mode of private VLAN

Examples

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode private-vlan promiscuous
DES-7200(config-if)# switchport private-vlan mapping 22 add 23-25
```

Related commands

Command	Description
show vlan private-vlan	

Platform description	The software version must be firmware v10.1 and later.

8.1.8 switchport private-vlan promiscuous trunk

Use this command to configure the ports as a promiscuous trunk port , which is associated with the L2 port and the private VLAN. Multiple pairs are allowed to associate.

[no] switchport private-vlan promiscuous trunk *p_vid_s_list*

Parameter description

Parameter	Description
p_vid	Primary VID
svlist	Secondary VLAN list.
no	Remove all the relationships between the layer-2 ports and private VLANs.

Default configuration	None.
Command mode	Interface configuration mode

Examples

```
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# switchport private-vlan promiscuous trunk 202 203
```

Related commands

Command	Description
-	-

Platform description The software version must be firmware v10.4 (3) and later.

8.2 Showing Related Commands

8.2.1 show vlan private-vlan

Show the configuration of private VLAN.

show vlan private-vlan [**community** | **primary** | **isolated**]

Parameter description

Parameter	Description
primary	Show the primary VLAN information.
community	Show the community VLAN information.
isolated	Show the isolated VLAN information.

Default configuration No private VLAN is configured.

Command mode Privileged mode.

Examples

```
DES-7200# show vlan private-vlan
```

Platform description The software version must be firmware v10.1 and later.

8.3 Hybrid Commands

8.3.1 switchport mode hybrid

Use this command to configure the port as a hybrid port.

switchport mode hybrid

no switchport mode

Parameter description

Parameter	Description
no	Delete the hybrid port.

Default configuration No hybrid port is configured.

Command mode Interface configuration mode.

Examples

```
DES-7200(config-if)# switchport mode hybrid
```

Platform description The software version must be firmware v10.1 and later.

8.3.2 switchport hybrid native vlan

Use this command to configure the default VLAN of a hybrid port.

switchport hybrid native vlan *vid*

no switchport hybrid native vlan

Parameter description

Parameter	Description
no	Restore the hybrid port to the default VLAN.

Default configuration No default VLAN is configured.

Command mode Interface mode.

Examples

```
DES-7200(config-if)# switchport hybrid native vlan 3
```

Platform description The software version must be firmware v10.1 and later.

8.3.3 switchport hybrid allowed vlan

Use this command to configure the output rules of a hybrid port.

switchport hybrid allowed vlan [[add] [tagged | untagged] | remove] v*list*

no switchport hybrid allowed vlan

Parameter description

Parameter	Description
no	Restore the output rules of the hybrid port to the default settings.

Default configuration No output rules are configured.

Command mode Interface mode.

Examples

```
DES-7200(config-if)# switchport hybrid allowed vlan add untagged 3-5
```

Platform description The software version must be firmware v10.1 and later.

9 Share VLAN Configuration Commands

9.1 Configuration Related Commands

9.1.1 share

Use this command to set the share vlan.

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

VLAN configuration mode.

Usage guidelines

Use the **no share** command to cancel the share vlan.

Enter the **end** command or **Ctrl+C** to return to the privileged EXEC mode.

Enter the **exit** command to return to the global configuration mode.

Examples

```
DES-7200(config)# vlan 2
DES-7200(config-vlan)# share
```

Related commands

Command	Description
-	-

9.2 Showing Related Commands

9.2.1 show mac-address-table share

Use this command to show the mac address status: original, duplicated and null. The “null” item indicates that share vlan has not been configured.

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Any configuration mode.

Usage guidelines

Enter the **end** command or **Ctrl+C** to return to the privileged EXEC mode.

Enter the **exit** command to return to the global configuration mode.

Examples

```
DES-7200# show mac-address-table share
Vlan  MAC Address     Type    Interface   Status
----  -------------- ------- ----------- ----------
   1   0040.4650.1e1e DYNAMIC Gigabit 0/1 original
   2   0040.4650.1e1e DYNAMIC Gigabit 0/1 duplicated
```

Related commands

Command	Description
-	-

10 MSTP Configuration Commands

10.1 Configuration Related Commands

10.1.1 spanning-tree

Use this command to enable MSTP and configure its basic settings globally. The **no** form of the command disables the spanning-tree function. The **no** form of the command with parameters only restores the corresponding parameters to the default values, but does not disable the spanning-tree function.

spanning-tree [**forward-time** *seconds*|**hello-time** *seconds* |**max-age** *seconds*]

no spanning-tree [**forward-time** | **hello-time** | **max-age**]

Parameter description

Parameter	Description
forward-time *seconds*	Interval at which the port status changes
hello-time *seconds*	Interval at which the switch sends the BPDU message
max-age *seconds*	Maximum aging time of the BPDU message

Default configuration Disabled.

Command mode Global configuration mode.

Usage guidelines	The values of **forward-time, hello time** and **max-age** are interrelated. Modifying one of these three parameters will affect the others. There is a restricted relationship among the above three values. 2*(Hello Time+1.0snd) <= Max-Age Time <= 2*(Forward-Delay–1.0snd) If the values do not according with the condition, the settings do not work.

Examples	Enable the spanning-tree function:
	`DES-7200(config)# spanning-tree`
	Configure the BridgeForwardDelay:
	`DES-7200(config)# spanning-tree forward-time 10`

Related commands

Command	Description
show spanning-tree	Show the global STP configuration.
spanning-tree mst cost	Set the PathCost of an STP interface.
spanning-tree tx-hold-count	Set the global TxHoldCount of STP.

10.1.2 spanning-tree bpdufilter

Use this command to enable BPDU filter on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU filter function on the interface.

spanning-tree bpdufilter [**enabled** | **disabled**]

Parameter description

Parameter	Description
enabled	Enable BPDU filter on the interface.
Disabled	Disable BPDU filter on the interface.

Default configuration	Disabled.
Command mode	Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# spanning-tree bpdufilter enable
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

10.1.3 spanning-tree bpduguard

Use this command to enable the BPDU guard function on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU guard function on the interface.

spanning-tree bpduguard [**enabled** | **disabled**]

Parameter description

Parameter	Description
enabled	Enable BPDU guard on the interface.
disabled	Disable BPDU guard on the interface.

Default configuration Disabled.

Command mode Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# spanning-tree bpduguard enable
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

10.1.4 spanning-tree link-type

Use this command to configure the link type of the interface. Use the **no** form of the command to restore the configuration to the default value.

spanning-tree link-type [**point-to-point** | **shared**]

no spanning-tree link-type

Parameter description

Parameter	Description
point-to-point	Set the link type of the interface to point-to-point.
shared	Forcibly set the link type of the interface to shared.

Default configuration

For a full-duplex interface, its link type is set to point-to-point link; for a half-duplex interface, its link type is set to shared.

Command mode

Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# spanning-tree link-type
point-to-point
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

10.1.5 spanning-tree max-hops

Use this command to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode, the number of hops in a region that the BPDU message passes before being dropped. This parameter takes effect for all instances. Use the **no** form of the command to restore it to the default setting.

spanning-tree max-hops *hop-count*

no spanning-tree max-hops

Parameter description

Parameter	Description
hop-count	Number of hops in a region that the BPDU message passes before being dropped. The range is 1 to 40 hops.

Default configuration

The default is 20 hops.

Command mode	Global configuration mode.
Usage guidelines	In the region, the BPDU message sent by the root bridge includes a Hot Count field. When the BPDU message passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates the BPDU message times out. The device will drop the BPDU message whose Hop Count is 0. Changing the **max-hops** command affects all instances.
Examples	This example shows how to set the max-hops of the spanning tree to 10 for all instances: `DES-7200(config)# spanning-tree max-hops 10` You can verify your setting by entering the **show spanning-tree mst** command in the privileged configuration mode.

Related commands

Command	Description
show spanning-tree	Show the MSTP information.

10.1.6 spanning-tree mode

Use this command to set the STP version in the global configuration mode. Use the **no** form of the command to restore the version of the spanning-tree to the default setting.

spanning-tree mode [**stp** | **rstp** | **mstp**]

no spanning-tree mode

Parameter description

Parameter	Description
stp	Spanning tree protocol(IEEE 802.1d)
rstp	Rapid spanning tree protocol(IEEE 802.1w)
mstp	Multiple spanning tree protocol(IEEE 802.1s)

Default	MSTP version.

configuration	
Command mode	Global configuration mode.
Examples	`DES-7200(config)# spanning-tree mode stp`

Related commands

Command	Description
show spanning-tree	Show the spanning-tree configuration.

10.1.7 spanning-tree mst configure

Use this command to enter the MST configuration mode in the global configuration mode and configure the MSTP region. Use the **no** form of the command to restore all parameters (name, revision, vlan map) to the default values.

spanning-tree mst configuration

no spanning-tree mst configuration

Default configuration	By default, all VLANs are mapped to the instance 0,*name* is empty, and *revision* is 0.
Command mode	Global configuration mode.
Usage guidelines	To return to the privileged EXEC mode, enter **end** or **Ctrl+C.** To return to the global configuration mode, enter **exit**. After entering the MST configuration mode, you can use the following commands to configure parameters: **instance** *instance-id* **vlan** *vlan-range*: Adds the VLANs to the MST instance. The range of *instance-id* is 0 to 64 and the range of VLAN is 1 to 4095. The *vlan-range* can be a collection of some inconsecutive VLANs separated with comma or some consecutive VLANs in the form of start VLAN number–end VLAN number. For example, **instance 10 vlan 2,3,6-9** means that VLANs 2, 3, 6, 7, 8, 9 are added to instance 10. By default, all VLANs are in Instance0. To remove a VLAN from an instance, use the

no form of the command: **no instance** *instance-id* [**vlan** *vlan-range*]. (In this case, the range of instance is 1 to 64).

name *name*: Specify the MST name, a string of up to 32 characters. You can use the **no name** command to restore it to the default setting.

revision *version*: Set the MST versions in the range 0 to 65535. You can use the **no name** command to restore it the default setting.

Show: Shows the information of the MST region.

Examples

This example shows how to enter the MST configuration mode, and map VLANs 3. 5 to 10 to MST instance 1:

```
DES-7200(config)# spanning-tree mst configuration
DES-7200(config-mst)# instance 1 vlan  3, 5-10
DES-7200(config-mst)# name region 1
DES-7200(config-mst)# revision  1
DES-7200(config-mst)# show
MST configuration
Name [region1]
Revision 1
Instance  Vlans Mapped
----------  --------------------
0       1-2,4,11-4094
1       3,5-10
---------------------------------
DES-7200(config-mst)# exit
DES-7200(config)#
```

To remove VLAN 3 from instance 1, execute this command after entering the MST configuration mode:

```
DES-7200(config-mst)# no instance 1 vlan 3
```

Delete instance 1:

```
DES-7200(config-mst)# no instance 1
```

You can verify your settings by entering the **show** command of the MST configuration commands.

Related commands

Command	Description
show spanning-tree mst	Show the MST region configuration.
instance *instance-id* **vlan** *vlan-range*	Add VLANs to the MST instance.
name	Configure the name of MST.
revision	Configure the version of MST.

	show	Show the MST mode in the MST configuration mode.

10.1.8 spanning-tree mst cost

Use this command to set the path cost of an instance in the interface configuration mode. Use the **no** form of the command to restore it to the default setting.

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] *cost*

Parameter description

Parameter	Description
instance-id	Instance ID in the range of 0 to 64
cost	Path cost in the range of 1 to 200,000,000

Default configuration

The default instance-id is 0.

The default value is calculated by the link rate of the interface automatically.

- 1000 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

Command mode

Interface configuration mode.

Usage guidelines

A higher cost value means a higher path cost.

Examples

This example shows how to set the path cost to 400 on the interface associated with instances 3:

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# spanning-tree mst 3 cost 400
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* command in the privileged EXEC mode.

Related

Command	Description

show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst port-priority	Configure the priority of an interface.
spanning-tree mst priority	Configure the priority of an instance.

10.1.9 spanning-tree mst port-priority

Use this command to configure the interface priority for different instances in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. Use the **no** form of the command to restore it to the default setting.

spanning-tree [**mst** *instance-id*] **port-priority** *priority*

no spanning-tree [**mst** *instance-id*] **port-priority**

Parameter description

Parameter	Description
Instance-id	Instance ID in the range of 0 to 64
priority	Interface priority. Sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, which are the multiples of 16.

Default configuration

The default instance-id is 0.

The default priority is 128.

Command mode

Interface configuration mode.

Usage guidelines

When a loop occurs in the region, the interface of the higher priority will be in charge of forwarding. If all interfaces have the same priority value, the interface of the smaller number will be in charge of the forwarding.

Examples

This example shows how to set the priority of **gigabitethernet 1/1** to 10 in instance 20:

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# spanning-tree mst 20 port-priority 0
```

	You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged command.

Related commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst cost	Set the path cost.
spanning-tree mst priority	Set the device priority for different instances.

10.1.10 spanning-tree mst priority

Use this command to set the device priority for different instances in the global configuration mode. Use the **no** form of the command to restore it to the default setting.

spanning-tree [**mst** *instance-id*] **priority** *priority*

no spanning-tree [**mst** *instance-id*] **priority**

Parameter description

Parameter	Description
instance-id	Instance ID in the range of 0 to 64
priority	Device priority. Sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152,53248, 57344 and 61440, which are all multiples of 4096.

Default configuration	The default instance ID is 0. The default device priority is 32768.
Command mode	Global configuration mode.

Examples	The following example sets the device priority of the Instance as 8192. `DES-7200(config-if)# spanning-tree mst 20 priority 8192` You can verify your settings by entering the **show spanning-tree mst** instance **interface** *instance-id* command in the privileged EXEC mode.

Related commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst cost	Set path cost.
spanning-tree mst port-priority	Set the port priority of an instance.

10.1.11 spanning-tree reset

Use this command to restore the **spanning-tree** configuration to the default value. This command does not have the **no** form.

spanning-tree reset

Parameter description	N/A.
Command mode	Global configuration mode.
Examples	`DES-7200(config)# spanning-tree reset`

Related commands

Command	Description
show spanning-tree	Show the global STP configuration.
show spanning-tree interface	Show the STP configuration of the interface.

10.1.12 spanning-tree tx-hold-count

Use this command to configure the TxHoldCount of the STP in the global configuraiton mode, the maximum number of the BPDU messages sent in one second. Use the **no** form of the command to restore it to the default setting.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

Parameter description

Parameter	Description
tx-hold-count	Maximum number of the BPDU messages sent in one second in the range 1 to 10.

Default configuration The default value is 3.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# spanning-tree tx-hold-count 5
```

Related commands

Command	Description
show spanning-tree	Show the global MSTP configuration.

10.1.13 spanning-tree pathcost method

Use this command to configure the path cost of the port. Use the **no** form of the command to restore it to the default setting.

spanning-tree pathcost method [**long [standard]** | **short**]

no spanning-tree pathcost method

Parameter description

Parameter	Description
Long [standard]	Adopt the 802.1t standard to configure path cost. The standard indicates that use the expression recommended by the standard to calculate the cost value.
short	Adopt the 802.1d standard to configure path cost.

Default configuration Adopt the 802.1T standard to set path cost by default.

Command mode	Global configuration mode.

Examples

```
DES-7200(config-if)# spanning-tree pathcost method long
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

10.1.14 spanning-tree portfast

Use this command to enable the portfast on the interface. You can use the **disabled** option of this command to disable the portfast feature on the interface.

spanning-tree portfast [**disabled**]

Parameter description

Parameter	Description
disabled	Disable the portfast on the interface.

Default configuration	Disabled.
Command mode	Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# spanning-tree portfast
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

10.1.15 spanning-tree portfast bpduguard default

Use this command to enable the GPDU guard globally. You can use the **no** form of the command to disable the BPDU guard.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Once the BPDU guard is enabled on the interface, it will enter the error-disabled status if the BPDU message arrives at the interface. Use the **show spanning-tree** command to display the configuration.
Examples	`DES-7200(config)# spanning-tree portfast bpduguard default`

Related commands

Command	Description
show spanning-tree interface	Show the global STP configuration.

10.1.16 spanning-tree portfast bpdufilter default

Use this command to enable the BPDU filter function globally. You can use the **no** form of the command to disable the BPDU filter.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.

Usage guidelines	Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the interface. Use the **show spanning-tree** command to display the configuration.
Examples	`DES-7200(config)# spanning-tree portfast bpdufilter default`

Related commands

Command	Description
show spanning-tree interface	Show the global STP configuration.

10.1.17 spanning-tree portfast default

Use this command to enable the portfast feature on all interfaces globally. Use the **no** form of the command to disable the portfast on all interfaces globally.

spanning-tree portfast default

no spanning-tree portfast default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7200(config)# spanning-tree portfast default`

Related commands

Command	Description
show spanning-tree interface	Show the global STP configuration.

10.1.18 spanning-tree tc-protection

Use this command to enable **tc-protection** globally. Use The **no** form of this command to disable **tc- protection** globally.

spanning-tree tc- protection

no spanning-tree tc- protection

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Global configuration mode.
Examples	`DES-7200(config)# spanning-tree tc-protection`

10.1.19 spanning-tree tc-protection tc-guard

Use this command to enable **tc-guard** globally to prevent the spread of TC messages. Use the **no** form of this command to disable **tc-guard** globally.

spanning-tree tc- protection tc-guard

no spanning-tree tc- protection tc-guard

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7200(config)# spanning-tree tc- protection tc-guard`

10.1.20 spanning-tree tc-guard

Use this command to enable **tc-guard** on the interface to prevent the spread of TC messages. Use the **no** form of this command to disable **tc-guard** on the interface.

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter description	N/A.

Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7200(config)# spanning-tree tc-guard`

10.1.21 spanning-tree ignore tc

Use this command to turn on the tc filtering switch on the interface. Use the **no** form of this command to turn off the tc filtering switch on the interface. With tc filtering enabled, the TC packets received on the interface will not be processed.

spanning-tree ignore tc

no spanning-tree ignore tc

Parameter description	N/A.
Default configuration	By default, the TC filtering function is enabled.
Command mode	Interface configuration mode.
Examples	`DES-7200(config-if)# spanning-tree ignore tc`

10.1.22 spanning-tree guard root

Use this command to enable **root guard** on the interface to prevent the change of current root bridge position because of error configuration and illegal packet attack. Use the **no** form of this command to disable **root guard** on the interface.

spanning-tree guard root

no spanning-tree guard root

Parameter description	N/A.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7200(config)# spanning-tree guard root`

10.1.23 spanning-tree loopguard default

Use this command to enable **loop guard** globally to prevent the root port or backup port from generating loop since they can not receive bpdu. Use the **no** form of this command to disable **loop guard**.

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7200(config)# spanning-tree loopguard default`

10.1.24 spanning-tree guard loop

Use this command to enable **loop guard** on the interface to prevent the root port or backup port from generating loop since they can not receive bpdu. Use the **no** form of this command to disable **loop guard**.

spanning-tree guard loop

no spanning-tree guard loop

Parameter description	N/A.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7200(config)# spanning-tree guard loop`

10.1.25 spanning-tree guard none

Use this command to disable **guard** on the interface. Use the **no** form of this command to delete **guard** on the interface.

spanning-tree guard none

no spanning-tree guard none

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7200(config)# spanning-tree guard none`

10.1.26 spanning-tree autoedge

Use this command to enable Autoedge on the interface. Use the **disabled** option of this command to disable Autoedge on the interface.

spanning-tree autoedge [**disabled**]

Parameter description	The **disabled** parameter is used to disable **Autoedge** on the interface.
Default configuration	Enabled.

Command mode	Interface configuration mode.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# spanning-tree autoedge disabled`

Related commands

Command	Function
show spanning-tree interface	Show the STP configuration information of the interface.

10.1.27 bpdu src-mac-check

Use this command to enable the BPDU source MAC address check function on the interface. Use the **no** form of this command to disable the function.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

Parameter description

Parameter	Description
H.H.H	Indicate that only the BPDU messages from this MAC address are received.
no	Indicate that the BPDU messages from any MAC address are received.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# bpdu src-mac-check 00d0.f800.1e2f`

10.1.28 clear spanning-tree detected-protocols

Use this command to force the interface to send the RSTP BPDU message and check the BPDU messages.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter description

Parameter	Description
interface-id	ID of the interface

Default configuration N/A.

Command mode Privileged configuration mode.

Examples

```
DES-7200# clear spanning-tree detected-protocols
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

10.1.29 spanning-tree compatible enable

Use this command to send the message selectively carried with MSTI according to the interface attibute of current port to realize interconnection with other vendors.

spanning-tree compatible enable

no spanning-tree compatible enable

Parameter description N/A.

Default configuration Disabled.

Command mode Interface configuration mode.

Examples

```
DES-7200(config)# spanning-tree compatible enable
```

10.2 Showing Related Command

10.2.1 show spanning-tree

Use this command to display the global spanning-tree configurations.

show spanning-tree [**summary** |**forward-time** | **hello-time** | **max-age** | **inconsistentports | tx-hold-count** | **pathcost** *method* | *max_hops*]

Parameter description

Parameter	Description
summary	Show the information of MSTP instances and forwarding status of the interfaces.
inconsistentports	Show the block port due to root guard or loop guard.
forward-time	Show BridgeForwardDelay.
hello-time	Show BridgeHelloTime.
max-age	Show BridgeMaxAge.
max-hops	Show the maximum hops of an instance.
tx-hold-count	Show TxHoldCount.
pathcost *method*	Show the method used for calculating path cost.

Command mode

Privileged EXEC mode.

Examples

```
DES-7200# show spanning-tree hello-time
```

Related commands

Command	Description
spanning-tree pathcost method	Set the pathcost method.
spanning-tree forward-time	Set BridgeForwardDelay.
spanning-tree hello-time	Set BridgeHelloTime.
spanning-tree max-age	Set BridgeMaxAge.
spanning-tree max-hops	Set the maximum hops of an instance.

	spanning-tree tx-hold-count	Show TxHoldCount.

10.2.2 show spanning-tree interface

Use this command to show the STP configuration of the interface, including the optional spanning tree.

show spanning-tree interface *interface-id* [{**bpdufilter** | **portfast** | **bpduguard** | **link-type** }]

Parameter description

Parameter	Description
interface-id	Interface ID
bpdufilter	Show the status of BPDU filter.
portfast	Show the status of portfast.
bpduguard	Show the status of BPDU guard.
link-type	Show the link type of an interface.

Command mode

Privileged EXEC mode.

Examples

```
DES-7200# show spanning-tree interface gigabitethernet 1/5
```

Related commands

Command	Description
spanning-tree bpdufilter	Enable the BPDU filter feature someone the interface.
spanning-tree portfast	Enable the portfast on the interface.
spanning-tree bpduguard	Enable the BPDU guard on the interface.
spanning-tree link-type	Set the link type of the interface to point-to-point.

10.2.3 show spanning-tree mst

In privileged EXEC mode, use this command to display the information of MST and instances.

show spanning-tree mst {**configuration** |*instance-id* [**interface** *interface-id*] }

Parameter description

Parameter	Description
configuration	The MST configuration of the

	equipment.
instance-id	Instance number
interface-id	Interface number

Default configuration

All the instances are displayed by default.

Command mode

Privileged mode.

Examples

```
DES-7200# show spanning-tree mst configuration
```

Related commands

Command	Description
spanning-tree mst configuration	Configure the MST region.
spanning-tree mst cost	Show the path cost of the instance.
spanning-tree mst max-hops	Show the maximum hops of the instance.
spanning-tree mst priority	Show the equipment priority of the instance.
spanning-tree mst port-priority	Show the port priority of the instance.

11 GVRP Configuration Commands

11.1 Configuration Related Command

11.1.1 gvrp applicant state

Use this command to set the port advertising mode, which determines whether to allow sending the GVRP advertisement on the port. Use the **no** form of this command to restore it to the default setting.

gvrp applicant state {**normal** | **non-applicant**}

no gvrp applicant state

Parameter description

Parameter	Description
-	-

Default Allow sending the GVRP advertisement on the port.

Command mode Interface configuration mode.

Usage guidelines Use the **show gvrp configuration** to show the related configurations.

Examples

```
DES-7200(config-if)# gvrp applicant state normal
```

Related commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

11.1.2 gvrp dynamic-vlan-creation

Use this command to control whether to allow creating the vlan dynamically. Use the **no** form of this command to restore it to the default setting. .

gvrp dynamic-vlan-creation enable

no gvrp dynamic-vlan-creation enable

Parameter description

Parameter	Description
-	-

Default Creating the vlan dynamically is not allowed.

Command mode Global configuration mode.

Usage guidelines Use the **show gvrp configuration** to show the related configurations.

Examples

```
DES-7200(config)# gvrp dynamic-vlan-creation enable
```

Related commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

11.1.3 gvrp enable

Use this command to enable the GVRP function. Use the **no** form of this command to restore it to the default setting.

gvrp enable

no gvrp enable

Parameter description

Parameter	Description
-	-

Default Disabled.

Command mode Global configuration mode.

Usage guidelines	Use the **show gvrp configuration** to show the related configurations.
Examples	`DES-7200(config)#gvrp enable`

Related commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

11.1.4 gvrp registration mode

Use this command to set the registration mode to control whether to allow creating/registering/canceling the vlan dynamically on the port. Use the **no** form of this command to restore it to the default setting.

gvrp registration mode {**normal** | **disabled**}

no gvrp registration mode

Parameter description

Parameter	Description
-	-

Default	Creating/registering/canceling the vlan dynamically is allowed.
Command mode	Interface configuration mode.
Usage guidelines	Use the **show gvrp configuration** to show the related configurations.
Examples	`DES-7200(config-if)# gvrp registration mode normal`

Related commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

11.1.5 gvrp timer

Use this command to set the GVRP timer. Use the **no** form of this command to restore it to the default setting.

gvrp timer {**join** | **leave** | **leaveall**} *timer_value*

no gvrp timer

Parameter description

Parameter	Description
join *timer_value*	Control the maximum delay before sending the advertisement on the port. The actual sending interval is in the range of 0 to the maximum delay.
leave *timer_value*	Control the waiting time before removing the VLAN from the port with the Leave Message received. If the Join Message is received again within this time range, the port-VLAN relation is still exist and the timer becomes invalid. If no Join Message is received on the port, the port status will be the Empty and removed from the VLAN member list.
leave all *timer_value*	Control the minimum interval of sending the LeaveAll Message on the port. If the LeaveAll Message is received before the timer expires, the timer re-counts. If the timer expires, send the LeaveAll Message on the port and also send this Message to the port, so that the Leave timer begins counting. The actual sending interval is ranging from leaveall to leaveall+join.

Default

Join timer: 200ms;
Leave timer: 600ms;
Leaveall timer: 10000ms.

Command mode

Global configuration mode.

Usage guidelines	Use the **show gvrp configuration** to show the related configurations.
Examples	`DES-7200(config)# gvrp timer join 200`

Related commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

11.2 Showing Related Commands

11.2.1 clear gvrp statistic

Use this command to clear the GVRP statistics for re-counting.

clear gvrp statistics { *interface-id* | **all**}

Parameter description

Parameter	Description
interface-id	Interface id.

Default	NA
Command mode	Privileged mode.
Usage guidelines	Use the **show gvrp statistics** to show the statistics.
Examples	`DES-7200# clear gvrp statistics all`

Related commands

Command	Description
show gvrp statistics	Show the GVRP statistics.

11.2.2 show gvrp configuration

Use this command to show the GVRP configurations.

show gvrp configuration

Parameter description

Parameter	Description
-	-

Default

NA

Command mode

Privileged mode.

Usage guidelines

Use the **show gvrp configuration** to show the related configurations.

Examples

```
DES-7200# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Join Timers(ms):600
Join Timers(ms):10000
Port based GVRP Configuration:
Port:GigabitEthernet 3/1 app mode:normal reg mode:normal
Port:GigabitEthernet 3/2 app mode:normal reg mode:normal
Port:GigabitEthernet 3/3 app mode:normal reg mode:normal
Port:GigabitEthernet 3/4 app mode:normal reg mode:normal
Port:GigabitEthernet 3/5 app mode:normal reg mode:normal
Port:GigabitEthernet 3/6 app mode:normal reg mode:normal
Port:GigabitEthernet 3/7 app mode:normal reg mode:normal
Port:GigabitEthernet 3/8 app mode:normal reg mode:normal
Port:GigabitEthernet 3/9 app mode:normal reg mode:normal
Port:GigabitEthernet 3/10 app mode:normal reg
mode:normal
Port:GigabitEthernet 3/11 app mode:normal reg
mode:normal
Port:GigabitEthernet 3/12 app mode:normal reg
mode:normal
```

Related

Command	Description

	-	-

11.2.3 show gvrp statistics

Use this command to show the GVRP statistics of one interface or all interfaces.

show gvrp statistics {*interface-id* | **all**}

Parameter description

Parameter	Description
interface-id	Interface id.

Default NA

Command mode Privileged mode.

Usage guidelines Use the **show gvrp statistics** to show the statistics of one interface or all interfaces.

Examples

```
DES-7200# show gvrp statistics gigabitethernet 1/1
Interface      GigabitEthernet 3/1
RecValidGvrpPdu        0
RecInvalidGvrpPdu      0
RecJoinEmpty    0
RecJoinIn      0
RecEmpty       0
RecLeaveEmpty   0
RecLeaveIn     0
RecLeaveAll    0
SentGvrpPdu    0
SentJoinEmpty   0
SentJoinIn     0
SentEmpty      0
SentLeaveEmpty  0
SentLeaveIn    0
SentLeaveAll   0
JoinIndicated   0
LeaveIndicated  0
JoinPropagated  0
```

```
LeavePropagated  0
```

Related commands

Command	Description
clear gvrp statistics	Clear the statistics of one interface or all interfaces.

11.2.4 show gvrp status

Use this command to show the GVRP status.

show gvrp status

Parameter description

Parameter	Description
-	-

Default NA

Command mode Privileged mode.

Usage guidelines Use the **show gvrp status** command to show the GVRP status.

Examples

```
DES-7200# show gvrp status
```

Related commands

Command	Description
-	-

12 QinQ Configuration Commands

12.1 Configuration Related Commands

12.1.1 dot1q outer-vid *vid* register inner-vid *v_list*

Use this command to configure the add policy list of outer vid based on protocol on tunnel port.

dot1q outer-vid *vid* **register inner-vid** *v_list*

no dot1q outer-vid *vid* **register inner-vid** *v_list*

Parameter description

Parameter	Description
v_list	Inner vlan id list
vid	Outer vlan id list
no	Remove the settings.

Default configuration

N/A.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring vid in the tag of input message as 4-22,adding the vid in the tag as 3:

```
DES-7200#configure
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#switchport mode dot1q-tunnel
DES-7200(config-if)#dot1q outer-vid 3 register inner-vid
4-22
DES-7200(config-if)#end
```

Related

Command	Description

	show registration-table [**interface** *intf-id*]	

Platform description	The software version must be firmware v10.3 and later.

12.1.2 dot1q relay-vid *vid* translate local-vid *v-list*

Use this command to configure the modify policy list of outer vid based on protocol on access，trunk，hybrid port.

dot1q relay-vid *vid* **translate local-vid** *v-list*

no dot1q relay-vid *vid* **translate local-vid** *v-list*

Parameter description

Parameter	Description
v_list	Outer vlan list of input message
vid	Modified outer vlan id list
no	Remove the settings.

Default configuration	Null policy list.

Command mode	Interface configuration mode.

Examples

Here is an example of configuring vid in the outer tag of input message as 10-20,modifying the vid as 100:

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# dot1q relay-vid 100 translate
local-vid 10-20
DES-7200(config-if)# end
```

Related commands

Command	Description
show translation-table [**interface** *intf-id*]	

Platform description	The software version must be firmware v10.3 and later.

12.1.3 dot1q relay-vid *vid* translate inner-vid *v-list*

Use this command to configure the modify policy list of outer vid based on protocol on access，trunk，hybrid port.

dot1q relay-vid *vid* **translate inner-vid** *v-list*

no dot1q relay-vid *vid* **translate inner-vid** *v-list*

Parameter description

Parameter	Description
v_list	Outer vlan list of input message
vid	Modified outer vlan id list
no	Remove the settings.

Default configuration	Null policy list.
Command mode	Interface configuration mode.

Examples

Here is an example of configuring vid in the outer tag of input message as 10-20,modifying the vid as 100:

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode access
DES-7200(config-if)#  dot1q  relay-vid  100  translate
inner-vid 10-20
DES-7200(config-if)# end
```

Related commands

Command	Description
show translation-table [**interface** *intf-id*]	

Platform description	The software version must be firmware v10.4 and later.

12.1.4 dot1q new-outer-vlan vid translate old-outer-vlan vid inner-vlan v-list

Use this command to modify the policy list of outer vid based on the inner Tag VID and outer Tag VID on the access, trunk, hybrid, uplink port.

dot1q new-outer-vlan *vid* **translate old-outer-vlan** *vid* **inner-vlan** ***v-list***

no dot1q new-outer-vlan *vid* **translate old-outer-vlan** *vid* **inner-vlan** *v-list*

Parameter description

Parameter	Description
v_list	Vid list of the
vid	Vid of outer tag.
no	Remove the setting.

Default configuration

Null policy list.

Command mode

Interface configuration mode.

Usage guideline

N/A.

Examples

The following example modifies the vid to 3888 when the input packets inner tag vid

```
DES-7200(config)# vlan 1888, 3888
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# dot1q new-outer-vlan 3888 translate old-outer-vlan 1888 inner-vlan 2001-3000
DES-7200(config-if)# end
```

Related commands

Command	Description
show translate-table [**interface** *intf-id*]	

Platform description

The software version must be firmware v10.4 and later.

12.1.5 dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

Use this command to map the priority from the outer tag to the inner tag for the packets on the interface.

dot1q-tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*

no dot1q-tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*

Parameter description

Parameter	Description
no	Cancel the priority mapping of the packets on the interface.

Default configuration

N/A.

Command mode

Interface configuration mode.

Usage guideline

N/A.

Examples

Here is an example of configuring the priority mapping from the outer tag to the inner tag:

```
DES-7200# configure
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# dot1q-tunnel cos 3 remark-cos 5
DES-7200(config-if)# end
```

Related commands

Command	Description
show interface intf-name remark	

Platform description

The software version must be firmware v10.4 and later.

12.1.6 frame-tag tpid *tpid*

Use this command to set the manufacturer tpid.

frame-tag tpid <*tpid*>

no frame-tag tpid

Parameter description

Parameter	Description
no	Remove the setting.

Command mode

Interface configuration mode.

Examples

```
DES-7200(config)# interface g0/3
DES-7200(config-if)# frame-tag tpid 0x9100
DES-7200(config-if)# end
DES-7200# show frame-tag tpid
Port    tpid
------  ---------
Gi0/3     0x9100
```

Related commands

Command	Description
show frame-tag tpid	

Platform description

The software version must be firmware v10.1 and later.

12.1.7 inner-priority-trust enable

Use this command to copy the priority of the inner tag to the outer tag of the packets on the interface.

inner-priority-trust enable

no inner-priority-trust enable

Parameter description

Parameter	Description
no	Remove the settings.

Command mode

Interface configuration mode.

Examples

```
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# inner-priority-trust enable
```

Related commands	**Command**	**Description**
	show inner-priority-trust	

Platform description The software version is firmware v10.1 and later.

12.1.8 mac-address-mapping x source-vlan src-vlan-list destination-vlan dst-vlan-id

Use this command to copy the MAC address dynamically-learned from the source VLAN to the destination VLAN.

mac-address-mapping *x* **destination-vlan** *dst-vlan-id* **source-vlan** *src-vlan-list*

no mac-address-mapping *x* **destination-vlan** *dst-vlan-id* **source-vlan** *src-vlan-list*

Parameter description	**Parameter**	**Description**
	no	Cancel to copy the MAC address dynamically-learned from the source VLAN to the destination VLAN.

Command mode Interface configuration mode.

Examples

```
DES-7200#configure
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# mac-address-mapping 1 destination-vlan 5 source-vlan 1-3
DES-7200(config-if)#end
```

Related commands	**Command**	**Description**
	show interface mac-address-mapping x	

Platform description The software version is firmware v10.4 and later.

12.1.9 switchport mode dot1q-tunnel

Use this command to configure the interface as the dot1q-tunnel interface.

switchport mode dot1q-tunnel

no switchport mode

Parameter description

Parameter	Description
no	Delete the corresponding dot1q-tunnel interface configuration.

Default configuration

No dot1q-tunnel interface is configured.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring the interface as the dot1q-tunnel interface:

```
DES-7200(config)# interface gi 0/1
DES-7200(config-if)# switchport access vlan 22
DES-7200(config-if)# switchport mode dot1q-tunnel
DES-7200(config)# end
```

Related commands

Command	Description
show vlan	

Platform description

The software version must be firmware v10.1 and later.

12.1.10 switchport mode uplink

Use this command to configure the interface as a uplink port.

switchport mode uplink

no switchport mode

Parameter description

Parameter	Description
no	Remove the settings.

Default configuration	No uplink port is configured.
Command mode	Interface configuration mode.

Examples	Here is an example of configuring the interface as a uplink port.
	`DES-7200(config)# interface gigabitEthernet 0/1`
	`DES-7200(config-if)# switchport mode up-link`
	`DES-7200(config)# end`

Related commands

Command	Description
show vlan	

Platform description	The software version must be firmware v10.1 and later.

12.1.11 switchport dot1q-tunnel allowed vlan

Use this command to configure the allowed VLAN of dot1q-tunnel.

switchport dot1q-tunnel allowed vlan [**add**] {**tagged|untagged**} *v_list*

switchport dot1q-tunnel allowed vlan remove *v_list*

no switchport dot1q-tunnel allowed vlan

Parameter description

Parameter	Description
tagged	Tag-carried.
untagged	Not tag-carried.
v_list	vlan id list.
no	Remove the settings.

Default configuration	Allowed vlan 1，untagged.
Command mode	Interface configuration mode.
Examples	Here is an example of configuring vlan 3-6 of dot1q-tunnel

port as allowed VLAN and outputting the frame with tag:

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#switchport dot1q-tunnel allowed vlan tagged 3-6
DES-7200(config)#end
```

Related commands

Command	Description
show interface dot1q-tunnel	

Platform description

The software version must be firmware v10.3 and later.

12.1.12 switchport dot1q-tunnel native vlan

Use this command to configure the default vlan id of dot1q-tunnel.

switchport dot1q-tunnel native vlan *vid*

no switchport dot1q-tunnel native vlan

Parameter description

Parameter	Description
vid	Configure default vlan id.
no	Configure default vlan as 1.

Default configuration

Vlan 1

Command mode

Interface configuration mode.

Examples

Here is an example of configuring default vlan of dot1q-tunnel port as 8:

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#switchport dot1q-tunnel native vlan 8
DES-7200(config)#end
```

Related

Command	Description

	show interface dot1q-tunnel	

Platform description	The software version must be firmware v10.3 and later.

12.1.13 traffic-redirect access-group acl outer-vlan

Use this command to configure the modify policy list of outer vid based on flow on access，trunk，hybrid port.

traffic-redirect access-group *acl* **outer-vlan** *vid* **in**

no traffic-redirect access-group *acl* **outer-vlan**

Parameter description

Parameter	Description
acl	Flow matching.
vid	Modified outer vid list
no	Remove the settings.

Default configuration	Null policy list.
Command mode	Interface configuration mode.

Examples

Here is an example of configuring outer vid of input message whose source address is 1.1.1.1 as 3:

```
DES-7200# configure
DES-7200(config)#ip access-list standard 2
DES-7200(config-std-nacl)# permit host 1.1.1.1
DES-7200(config-std-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# traffic-redirect access-group 2
outer-vlan 3 in
DES-7200(config-if)# end
```

Related

Command	Description

	show traffic-redirect	

Platform description	The software version must be firmware v10.3 and later.

12.1.14 traffic-redirect access-group *acl* inner-vlan

Use this command to configure the modification policy of inner vid based on flow for the packets outputted from the access，trunk，hybrid port.

traffic-redirect access-group *acl* **inner-vlan** *vid* **out**

no traffic-redirect access-group *acl* **inner-vlan**

Parameter description

Parameter	Description
acl	Flow matching.
vid	Modified inner vid
no	Remove the settings.

Default configuration	None

Command mode	Interface configuration mode.

Examples

Here is an example of configuring the outer vid of outgoing messages whose source address is 1.1.1.2 as 6:

```
DES-7200#configure
DES-7200(config)#ip access-list standard to_6
DES-7200(config-std-nacl)#permit host 1.1.1.2
DES-7200(config-std-nacl)#exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# traffic-redirect access-group to_6
inner-vlan 6 out
DES-7200(config-if)# end
```

Related commands

Command	Description
show traffic-redirect	

Platform description	The software version must be firmware v10.3 and later.

12.1.15 traffic-redirect access-group acl nested-vlan

Use this command to configure vid add policy list based on flow on dot1q-tunne port.

traffic-redirect access-group *acl* **nested-vlan** *vid* **in**

no traffic-redirect access-group *acl* **nested –vlan**

Parameter description

Parameter	Description
acl	Flow matching.
vid	vid list to be added.
no	Remove the settings.

Default configuration	Null policy list.
Command mode	Interface configuration mode.

Examples

Here is an example of adding the vid of input message whose source address is 1.1.1.3 as 9:

```
DES-7200#configure
DES-7200(config)#ip access-list standard 20
DES-7200(config-std-nacl)#permit host 1.1.1.3
DES-7200(config-std-nacl)#exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode dot1q-tunnel
DES-7200(config-if)# traffic-redirect access-group 20
nested-vlan 10 in
DES-7200(config-if)# end
```

Related commands

Command	Description
show traffic-redirect	

Platform description	The software version must be firmware v10.1 and later.

12.1.16 l2protocol-tunnel

Use this command to set the dot1q-tunnel port to receive L2 protocol message.

l2protocol-tunnel {**stp | gvrp**}

no l2protocol-tunnel {**stp | gvrp**}

Parameter description

Parameter	Description
stp	Receive stp message.
gvrp	Receive gvrp message.
no	Remove the settings.

Command mode

Global configuration mode.

Examples

Here is an example of enabling the function of receiving L2 protocol gvrp and stp:

```
DES-7200#configure
DES-7200(config)# l2protocol-tunnel stp
DES-7200(config)# l2protocol-tunnel gvrp
DES-7200(config)#end
```

Related commands

Command	Description
show l2protocol-tunnel { gvrp | stp }	

Platform description

The software version must be firmware v10.3 and later.

12.1.17 l2protocol-tunnel *proto-type* enable

Use this command to enable transparent transmission of L2 protocol message.

l2protocol-tunnel {stp | gvrp} enable

no l2protocol-tunnel {stp | gvrp} enable

Parameter description

Parameter	Description
stp	Transparently transmit stp message.

	gvrp	Transparently transmit gvrp message.
	no	Remove the settings.

Command mode	Intereface configuration mode.

Examples	Here is an example of enabling transparent transmission of L2 protocol message ：
	`DES-7200#configure`
	`DES-7200(config)# interface fa 0/1`
	`DES-7200(config-if)# l2protocol-tunnel gvrp enable`
	`DES-7200(config-if)#end`

Related commands	**Command**	**Description**
	show l2protocol-tunnel {gvrp|stp}	

Platform description	The software version must be firmware v10.3 and later.

12.1.18 l2protocol-tunnel *proto-type* tunnel-dmac *mac-address*

Use this command to set the MAC address for the transparent transmission of the corresponding protocol messages.

l2protocol-tunnel { **stp|gvrp** } **tunnel-dmac mac-address**

no l2protocol-tunnel { **stp**|**gvrp** } **tunnel-dmac mac-address**

Parameter description	**Parameter**	**Description**
	stp	Set the STP transparent transmission address.
	gvrp	Set the GVRP transparent transmission address.
	no	Restore the transparent transimission address to the default value.

Command	Global configuration mode.

mode

Examples

Here is an example of setting the MAC address for the L2-protocol transparent transmission function:

```
DES-7200(config-if)# l2protocol-tunnel gvrp tunnel-dmac 011AA9 000005
DES-7200(config-if)#end
```

Related commands

Command	Description
show l2protocol-tunnel {gvrp|stp}	

Platform description

The software version must be firmware v10.4 and later.

12.2 Showing Commands

12.2.1 show dot1q-tunnel

Use this command to show whether dot1q-tunnel of interface is enabled or not.

show dot1q-tunnel [**interface** *intf-id*]

Parameter description

Parameter	Description
intf-id	The specified interface.

Default configuration

N/A.

Command mode

Privileged mode.

Examples

```
DES-7200# show dot1q-tunnel
Ports   Dot1q-tunnel
-----   ---------
Gi0/1     Enable
```

Platform description

The software version must be firmware v10.3 and later.

12.2.2 show frame-tag tpid

Use this command to show the configuration of interface tpid.

show frame-tag tpid [**interface <***intf-id***>**]

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration

The tpid is not modified.

Command mode

Privileged mode.

Examples

```
DES-7200# show frame-tag tpid
Ports    tpid
-----  ---------
Gi0/1     0x9100
```

Platform description

The software version must be firmware v10.1 and later.

12.2.3 show inner-priority-trust

Use this command to show the priority copy configuration.

show inner-priority-trust

Parameter description

N/A.

Default configuration

Priority copy is disabled by default.

Command mode

Privileged mode.

Examples

```
DES-7200# show inner-priority-trust
Port     inner-priority-trust
----    ----------
Gi0/1     enable
```

Platform description	The software version must be firmware v10.1 and later.

12.2.4 show interface dot1q-tunnel

Use this command to show dot1q-tunnel configuration.

show interface [*intf-id*] **dot1q-tunnel**

Parameter description

Parameter	Description
intf-id	The specified interface.

Default configuration	N/A.
Command mode	Privileged mode.

Examples

```
DES-7200# show interface dot1q-tunnel
Interface: Gi0/3
Native vlan: 10
Allowed vlan list: 4-6，10，30-60
Tagged vlan list: 4，6，30-60
```

Platform description	The software version must be firmware v10.3 and later.

12.2.5 show interface intf-name remark

Use this command to show the priority mapping configurations.

show interface intf-name remark

Parameter description

Parameter	Description
-	-

Default configuration	N/A.
Command mode	Privileged mode.

Examples

```
DES-7200# show interface intf-name remark
Ports        Type       From value  To value
------------ ---------- ----------- --------
Gi0/1        Cos-To-Cos  3           5
```

Platform description The software version must be firmware v10.1 and later.

12.2.6 show interface mac-address-mapping x

Use this command to show the mac address mapping configurations.

show interface mac-address-mapping x

Parameter description

Parameter	Description
-	-

Default configuration N/A.

Command mode Privileged mode.

Examples

```
DES-7200# show mac-address-mapping 1
Ports        Destination-VID  Source-VID-list
------------ ---------------- ---------------
Gi0/1        5                1-3
```

Platform description The software version must be firmware v10.1 and later.

12.2.7 show registration-table

Use this command to show vid add policy list of prorocol-based dot1q-tunnel port.

show registration-table [**interface** *intf-id*]

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration

Null policy list.

Command mode

Privileged mode.

Examples

```
DES-7200# show registration-table
Ports        Outer-VID  Inner-VID-list
------------ ---------- -----------------
Gi0/7        5          7-10,15,20-30
```

Platform description

The software version must be firmware v10.3 and later.

12.2.8 show traffic-redirect

Use this command to show flow-based vid change or add policy list.

show traffic-redirect [**interface** *intf-id*]

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration

Null policy list.

Command mode

Privileged mode.

Examples

```
DES-7200# show traffic-redirect
Ports           Type          VID   Match-filter
------------ ----------- ---- ------------
Gi0/3        Mod-outer   23   11
Gi0/3        Mod-outer   3    4
Gi0/3        Mod-outer   6    5
Gi0/3        Mod-inner   8    inner-to-8
Gi0/6        Mod-inner   9    100
```

```
Gi0/7        Nested-vid   13   nest-13
```

Platform description	The software version must be firmware v10.3 and later.

12.2.9 show translation-table

Use this command to show vid modify policy list of prorocol-based access, trunk, hybrid port.

show translation-table [**interface** *intf-id*]

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration	Null policy list.
Command mode	Privileged mode.

Examples

```
DES-7200# show translation-table
Ports        Relay-VID  Local-VID-list
------------ ---------- -----------------
Gi0/8        10         8-9,15,20-30
```

Platform description	The software version must be firmware v10.3 and later.

12.2.10 show l2protocol-tunnel

Use this command to show transparent transmission configuration of L2 protocol.

show l2protocol-tunnel { **gvrp | stp** }

Parameter description

Parameter	Description
gvrp	Show configuration of transparently transmitting gvrp protocol.
stp	Show configuration of transparently

		transmitting stp protocol.

Default configuration	N/A .
Command mode	Privileged mode.
Examples	DES-7200# show l2protocol-tunnel stp L2protocol-tunnel: Stp Enable DES-7200# show l2protocol-tunnel gvrp L2protocol-tunnel: gvrp Disable
Platform description	The software version must be firmware v10.3 and later.

DES-7200

IP Application Command Reference Guide

Version 10.4(3)

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 IP Address Configuration Commands

1.1 Interface Address Configuration Commands

1.1.1 ip-address

Use this command to configure the IP address of an interface. The **no** form of this command can be used to delete the IP address of the interface.

ip address *ip-address network-mask* [**secondary**] | [**gateway** *ip-address*]

no ip address [*ip-address network-mask* [**secondary**] | [**gateway**]]

Parameter description

Parameter	Description
ip-address	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.
network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.
secondary	Indicates the secondary IP address that has been configured.
gateway *ip-address*	Configure the gateway address for the layer-2 switch, which is only supported on the layer-2 switches. No address is followed by the gateway when using the no form of this command.

Default No IP address is configured for the interface.

Usage guidelines Interface configuration mode.

Usage The equipment cannot receive and send IP packets before

guidelines

it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value “1” are the network address. The IP address bits that correspond to value “0” are the host address. For example, the network mask of Class A IP address is “255.0.0.0”. You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The DES-7200 supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary IP addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses. The secondary IP address and the primary IP address must belong to the same network or different networks. Secondary IP addresses are often used in network construction. Typically, you can try to use secondary IP addresses in the following situations:

- A network hasn’t enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured.
- Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet.
- Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet

	cannot appear on two or more interfaces of a device.

Examples

In the example below, the primary IP address is configured as 10.10.10.1, and the network mask is configured as 255.255.255.0.

```
ip address 10.10.10.1 255.255.255.0
```

In the example below, the default gateway is configured as 10.10.10.254

```
ip address 10.10.10.1 255.255.255.0 gateway 10.10.10.254
```

Related commands

Command	Description
show interface	Show detailed information of the interface.

Platform description

For the Layer 2 switch, the IP address can be configured only for the Layer 3 interface. The Level-2 address is not supported, that is, the secondary option is unavailable.

The keyword **gateway** is only supported by the layer-2 switches.

1.1.2 ip unnumbered

Use this command to configure an unnumbered interface. After an interface is configured as unnumbered interface, it is allowed to run the IP protocol and can receive and send IP packets. The **no** form can be used to remove this configuration.

ip unnumbered *interface-type interface-number*

no ip unnumbered

Parameter description

Parameter	Description
interface-type	Interface type
interface-number	Interface number

Default N/A.

Command mode Interface configuration mode.

Usage guidelines

Unnumbered interface is an interface that has IP enabled on it but no IP address is assigned to it. The unnumbered interface should be associated to an interface with an IP address. The source IP address of the IP packet generated by an unnumbered interface is the IP address of the associated interface. In addition, the routing protocol process determines whether to send route update packets to an unnumbered interface according to the IP address of the associated interface. The following restrictions apply when an unnumbered interface is used:

- An Ethernet interface cannot be configured as an unnumbered interface.
- A serial interface can be configured as an unnumbered interface when it is encapsulated with SLIP, HDLC, PPP, LAPB and Frame-relay. However, when Frame-relay is used for encapsulation, only the point-to-point interface can be configured as an unnumbered interface. X.25 encapsulation does not allow configuration as an unnumbered interface.
- You cannot detect whether an unnumbered interface works normally using the **ping** command, because no IP address is configured for the unnumbered interface. However, the status of the unnumbered interface can be monitored remotely using SNMP.
- The network cannot be started using an unnumbered interface.

Examples

In the example below the local interface is configured as an unnumbered interface, and the associated interface is FastEthernet 0/1. An IP address must be configured for the associated interface.

```
ip unnumbered fastEthernet 0/1
```

Related commands

Command	Description
show interface	Show detailed information of the interface.

Platform description

This command is not supported on the Layer 2 switch.

1.2 Address Resolution Protocol (ARP) Configuration Commands

1.2.1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. The **no** form of this command deletes the static MAC address mapping.

arp *ip-address MAC-address type* [**alias**]

no arp *ip-address MAC-address type* [**alias**]

Parameter description

Parameter	Description
ip-address	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
MAC-address	48-bit data link layer address
type	ARP encapsulation type. The keyword is **arpa** for the Ethernet interface.
alias	(Optional) DES-7200 will respond to the ARP request from this IP address after this parameter is defined.

Default

There is no static mapping record in the ARP cache table.

Command mode

Global configuration mode.

Usage guidelines

DES-7200 finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table.

Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The **clear arp-cache** command can be used to delete the ARP mapping that is learned dynamically.

Examples

The following is an example of setting an ARP static mapping record for a host in the Ethernet.

```
arp 1.1.1.1 4e54.3800.0002 arpa
```

Related

Command	Description

	clear arp-cache	Clear the ARP cache table

1.2.2 arp anti-ip-attack

For the messages corresponds to the directly-connected route, if the switch does not learn the ARP that corresponds to the destination IP address, it is not able to forward the message in hardware, and it needs to send the message to the CPU to resolve the address(that is the ARP learnning). Sending large number of this messages to the CPU will influence the other tasks of the switch. To prevent the IP messages from attacking the CPU, a discarded entry is set to the hardware during the address resolution, so that all sequential messges with that destination IP address are not sent to the CPU. After the address resolution, the entry is updated to the forwarding status, so that the switch could forward the message with that destination IP address in hardware.

In general, during the ARP request ,if the switch CPU receives three destination IP address messages corresponding to the ARP entry, it is considered to be possilble to attack the CPU and the switch sets the discarded entry to prevent the unknown unicast message from attacking the CPU. User could set the *num* parameter of this command to decide whether it attacks the CPU in specific network environment or disable this function. Use the **arp anti-ip-attack** command to set the parameter or disable this function. The **no** form of this command restores it to default value 3.

arp anti-ip-attack *num*

no arp anti-ip-attack

	Parameter	**Description**
Parameter description	*num*	The number of the IP message to trigger the ARP to set the discarded entry in the range of 0 to 100. 0 stands for disabling the arp anti-ip-attack function.

Default configuration	By default, set the discarded entry after 3 unknown unicast messages are sent to the CPU.
Command mode	Global configuration mode.

Usage guidelines	The arp anti-ip-attack function needs to occupy the switch hardware routing resources when attacked by the unknown unicast message. If there are enough resources, the **arp anti-ip-attack** *num* could be smaller. If not, in order to preferential ensure the use of the normal routing, the *num* could be larger or disable this function.

Examples	The following configuration sets the IP message number that triggers to set the discarding entry as 5.
	`DES-7200(config)# arp anti-ip-attack 5`
	The following configuration disables the ARP anti-ip-attack function.
	`DES-7200(config)# arp anti-ip-attack 0`

Platform description	This command is supported on the Layer 3 switch.

1.2.3 arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface..The **no** form of this command disables this function on the interface.

arp gratuitous-send interval *seconds*

no arp gratuitous-send

Parameter description

Parameter	Description
seconds	The time interval to send the free ARP request message in the range 1 to 3600 seconds

Default configuration	This function is not enabled on the interface to send the free ARP request regularly.
Command mode	Interface configuration mode.

Usage guidelines	If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

Examples	The following configuration sets to send one free ARP request to SVI 1 per second.
	`DES-7200(config)# interface vlan 1`
	`DES-7200(config-if)# arp gratuitous-send interval 1`
	The following configuration stops sending the free ARP request to SVI 1.
	`DES-7200(config)# interface vlan 1`
	`DES-7200(config-if)# no arp gratuitous-send`

1.2.4 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. The **no** form of this command is used to restore the default value, that is, retry an ARP request per second.

arp retry interval *seconds*

no arp retry interval

Parameter description

Parameter	Description
seconds	Time for retrying the ARP request message in the range of 1 to 3600 seconds, 1 second by default.

Default configuration	The retry interval of the ARP request is 1s.
Command mode	Global configuration mode.
Usage guidelines	The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

Examples

The following configuration sets the retry interval of the ARP request as 30s.

```
arp retry interval 30
```

Related commands

Command	Function
arp retry times *number*	Set the retry time of the ARP request message.

1.2.5 arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. The **no** form of this command can be used to restore the default 5 times of the ARP retry requests.

arp retry times *number*

no arp retry times

Parameter description

Parameter	Description
number	The times of sending the same ARP request in the range 1 to100..When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent.

Default configuration

If the ARP response message is not received, the ARP request message will be sent for 5 times, and then it will be timed out.

Command mode

Global configuration mode.

Usage guidelines

The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

Examples

The following configuration will set the local ARP request not to be retried.

```
arp retry times 1
```

The following configuration will set the local ARP request to be retried for one time.

```
arp retry times 2
```

Related commands

Command	Function
arp retry interval *seconds*	Set the retry interval of the ARP request message.

1.2.6 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache. The no form of this command restores it to the default configuration.

arp timeout *seconds*

no arp timeout

Parameter description

Parameter	Description
seconds	The timeout ranging 0 to 2147483 seconds

Default The default timeout is 3600 seconds.

Command mode Interface configuration mode.

Usage guidelines

The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

Examples

The following is an example of setting the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet port 0/1 to 120 seconds.

```
interface fastEthernet 0/1
arp timeout 120
```

Related commands

Command	Description
clear arp-cache	Clear the ARP cache list.
show interface	Show the interface information.

1.2.7 arp trusted

Use this command to set the maximun number of trusted ARP entries.The **no** form of this command restores it to the default value.

arp trusted *number*

no arp trusted

Parameter description

Parameter	Description
number	Maximum number of trusted ARP entries in the range of 10 to 4096.

Default configuration

The default value is different for different products.

Command mode

Global configuration mode.

Usage guidelines

To make this command valid, enable the trusted ARP function firstly. The trusted ARP entries and other entries share the memory. Too much trusted ARP entries may lead to insufficient ARP entry space. In general, you should set the maximum number of trusted ARP entries according to your real requirements.

Examples

The following configuration sets 1000 trusted ARPs.

```
arp trusted 1000
```

Related commands

Command	Function
service trustedarp	Enable the trusted ARP function.

Platform description	N/A

1.2.8 arp unresolve

Use this command to configure the maximum number of the unresolved ARP entries. The **no** form of this command can restore it to the default value 8192.

arp unresolve *number*

no arp unresolve

Parameter description

Parameter	Description
number	The maximum number of the unresolved ARP entries in the range of 1 to 8192. The default value is 8192.

Default configuration	The ARP cache table can contain up to 8192 unresolved entries.
Command mode	Global configuration mode.
Usage guidelines	If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.
Examples	The following configuration sets the maximum number of the unresolved items as 500. `arp unresolve 500`

1.2.9 ip proxy-arp

Use this command to enable ARP proxy funtion on the interface. The **no** form of this command disables ARP function.

ip proxy-arp

no ip proxy-arp

Default	Disabled on the version higher than 10.2(3).

Command mode	Interface configuration mode.
Usage guidelines	Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

Examples	The following is an example of enabling ARP on FastEthernet port 0/1:
	`interface fastEthernet 0/1`
	`ip proxy-arp`

Platform description	This command is not supported on the Layer 2 switch.

1.2.10 service trustedarp

Use this command to enable the trusted ARP function.The **no** form of this command disables the trusted ARP function.

service trustedarp

no service trustedarp

Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The trusted ARP function of the device is to prevent the ARP fraud function. As a part of the GSN scheme, it should be used together with the GSN scheme. In the following three cases, the STP protocol clears not only the dynamic MAC address of a port but also the

trusted entries, including trusted MAC and trusted ARP:

1 STP is enabled.

2 The port is set to neither root port nor designed port. This may be caused when the port is up or down or the port priority is modified.

3 TC packet is received on the port, and the addresses of the ports not receiving PC packet are cleared.

Examples

The following configuration is to enable the trusted ARP function in the global configuration mode.

```
config
service trustedarp
```

Platform description

N/A

1.2.11 trusted-arp user-vlan

Use this command to execute the VLAN transformation while setting the trusted ARP entries.The **no** form of this command deletes an ARP entry.

trusted-arp user-vlan *vid1* **translated-vlan** *vid2*

no trusted-arp user-vlan *vid1*

Parameter description

Parameter	Description
vid1	VID set by the server.
vid2	VID after the transformation.

Default configuration

No VLAN transformation is executed.

Command mode

Global configuration mode.

Usage guidelines

In order to validate this command, enable the trusted ARP function first. This command is needed only when the VLAN sent by the server is different from the VLAN which takes effect in the trusted ARP entry.

Examples	The following configuration is to set the VLAN sent by the server to 3, but the VLAN which takes effect in the trusted ARP entry to 5. `trusted-arp user-vlan 3 translated-vlan 5`

Related commands

Command	Function
service trustedarp	Enable the trusted ARP function.

Platform description	N/A

1.3 Broadcast Message Processing Configuration Commands

1.3.1 ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. The **no** form of this command is used to remove the broadcast address configuration.

ip broadcast-addresss *ip-address*

no ip broadcast-addresss

Parameter description

Parameter	Description
ip-address	Broadcast address of IP network

Default	The default IP broadcast address is 255.255.255.255.
Command mode	Interface configuration mode.
Usage guidelines	At present, the destination address of IP broadcast packet is all “1”, represented as 255.255.255.255. The DES-7200 can generate broadcast packets with other IP addresses through definition, and can receive both all “1” and the broadcast packets defined by itself.
Examples	The following is an example of setting the destination

	address of IP broadcast packets generated by this interface to 0.0.0.0. `ip broadcast-address 0.0.0.0`
Platform description	This command is not supported on the Layer 2 switch.

1.3.2 ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. The **no** form of this command is used to remove the configuration.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter description

Parameter	Description
access-list-number	(Optional) Access list number ranging 1 to 199 and 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

Default	Disabled.
Command mode	Interface configuration mode.

Usage guidelines	IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet. The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all “1”), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast. You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets. You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast. If **no ip directed-broadcast** is configured on an interface, DES-7200 will discard the directed broadcast packets received from the directly connected network.

Examples	The following is an example of enabling forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device.
	`interface fastEthernet 0/1`
	`ip directed-broadcast`

Platform description	This command is not supported on the Layer 2 switch.

1.4 IP Address Monitoring and Maintenance Commands

1.4.1 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table in the privileged mode.

clear arp-cache [**vrf** *vrf_name* | **trusted**] [*ip* [*mask*]] | **interface** *interface-name*]

Command mode	Privileged mode.
Usage guidelines	This command can be used to refresh an ARP cache table.

Caution

On a NFPP-based(Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two **clear arp** times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.

Examples

The following is an example of removing all dynamic ARP mapping records.

```
clear arp-cache
```

The following is an example of removing dynamic ARP table entry 1.1.1.1

```
clear arp-cache 1.1.1.1
```

The following is an example of removing dynamic ARP table entry on interface SVI1

```
clear arp-cache interface Vlan 1
```

Related commands

Command	Description
arp	Add a static mapping record to the ARP cache table.

Platform description	N/A

1.4.2 clear ip route

Use this command to remove the entire IP routing table or a particular routing record in the IP routing table in the privileged user mode.

clear ip route { ***** **|** *network* [*netmask*] }

Parameter description

Parameter	Description
*	Remove all the routes.
network	The network or subnet address to be removed
netmask	(Optional) Network mask

Command mode

Privileged mode.

Usage guidelines

Once an invalid route is found in the routing table, you can immediately refresh the routing table to get the updated routes. Note that, however, refreshing the entire routing table will result in temporary communication failure in the entire network.

Examples

The example below refreshes only the route of 192.168.12.0.

```
clear ip route 192.168.12.0
```

Related commands

Command	Description
show ip route	Show the IP routing table.

Platform description

This command is not supported on the Layer 2 switch.

1.4.3 show arp

Use this command to show the Address Resolution Protocol (ARP) cache table

show arp [[**vrf** *vrf-name*] [**trusted**] *ip* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]

Parameter description

Parameter	Description
ip	Show the ARP entry of the specified IP address.

vrf *vrf-name*	VRF instance, which shows the ARP entry with specified VRF.
ip mask	Show the ARP entries of the network segment included within the mask.
mac-address	Show the ARP entry of the specified MAC address.
static	Show all the static ARP entries.
complete	Show all the resolved dynamic ARP entries.
incomplete	Show all the unresolved dynamic ARP entries.
mac-address	Show the ARP entry with the specified mac address.

Command mode

Any

Examples

The following is the output result of the **show arp** command:

```
DES-7200# show arp
Total Numbers of Arp: 7
Protocol  Address          Age(min)  Hardware        Type
Interface
Internet  192.168.195.68   0         0013.20a5.7a5f  arpa
VLAN 1
Internet  192.168.195.67   0         001a.a0b5.378d  arpa
VLAN 1
Internet  192.168.195.65   0         0018.8b7b.713e  arpa
VLAN 1
Internet  192.168.195.64   0         0018.8b7b.9106  arpa
VLAN 1
Internet  192.168.195.63   0         001a.a0b5.3990  arpa
VLAN 1
Internet  192.168.195.62   0         001a.a0b5.0b25  arpa
VLAN 1
Internet  192.168.195.5    --        00d0.f822.33b1  arpa
VLAN 1
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses
Interface	Interface associated with the IP addresses

The following is the output result of **show arp** *192.168.195.68*

```
DES-7200# show arp 192.168.195.68
Protocol  Address      Age(min)  Hardware           Type
Interface
Internet  192.168.195.68   1   0013.20a5.7a5f  arpa   VLAN 1
```

The following is the output result of **show arp** *192.168.195.0 255.255.255.0*

```
DES-7200# show arp 192.168.195.0 255.255.255.0
Protocol  Address    Age(min)  Hardware   Type   Interface
Internet  192.168.195.64   0   0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.2    1   00d0.f8ff.f00e  arpa   VLAN 1
Internet  192.168.195.5    --   00d0.f822.33b1  arpa   VLAN 1
Internet  192.168.195.1    0   00d0.f8a6.5af7  arpa   VLAN 1
Internet  192.168.195.51   1   0018.8b82.8691  arpa   VLAN 1
```

The following is the output result of **show arp** *001a.a0b5.378d*

```
DES-7200# show arp 001a.a0b5.378d
Protocol  Address  Age(min)  Hardware  Type   Interface
Internet  192.168.195.67   4   001a.a0b5.378d  arpa   VLAN 1
```

Platform description	N/A

1.4.4 show arp counter

Use this command to show the number of ARP entries in the ARP cache table.

show arp counter

Parameter description	N/A.
Command mode	Any.

Examples	The following is the output result of the **show arp counter** command:
	`DES-7200# show arp counter`
	`The Arp Entry counter:0`
	`The Unresolve Arp Entry:0`
	The meaning of each field in the ARP cache table is described in Table 1.

1.4.5 show arp detail

Use this command to show the details of the Address Resolution Protocol (ARP) cache table.

show arp detail [*interface-type interface-number*| *ip [mask]* | *mac-address* | **static | complete | incomplete**]

Parameter description

Parameter	Description
Interface-type interface-number	Show the ARP of the layer 2 port or the layer 3 interface.
ip	Show the ARP entry of the specified IP address.
ip mask	Show the ARP entries of the network segment included within the mask.
mac-address	Show the ARP entry of the specified MAC address.
static	Show all the static ARP entries.
complete	Show all the resolved dynamic ARP entries.
incomplete	Show all the unresolved dynamic ARP entries.

Command mode	Privileged mode
Usage guidelines	Use this command to show the ARP details, such as the ARP type (Dynamic, Static, Local, Trust), the information on the layer2 port.
Examples	The following is the output result of the **show arp detail** command:

```
DES-7200# show arp detail
IP Address        MAC Address        Type        Age(min)
Interface  Port
20.1.1.1          000f.e200.0001     Static      --     --
--
20.1.1.1          000f.e200.0001     Static      --     Vl3
--
20.1.1.1          000f.e200.0001     Static      --     Vl3
Gi2/0/1
193.1.1.70        00e0.fe50.6503     Dynamic     1      Vl3
Gi2/0/1
192.168.0.1      0012.a990.2241    Dynamic    10    Gi2/0/3
Gi2/0/3
192.168.0.1       0012.a990.2241     Dynamic     20     Ag1
Ag1
192.168.0.1       0012.a990.2241     Dynamic     30     Vl2
Ag2
192.168.0.39      0012.a990.2241     Local       --     Vl3
--
192.168.0.39     0012.a990.2241    Local      --    Gi2/0/3
--
192.168.0.1       0012.a990.2241     Local       --     Vl3
--
192.168.0.1      0012.a990.2241    Local      --    Gi2/3/2
--
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
IP Address	IP address corresponding to the hardware address

MAC Address	hardware address corresponding to the IP address
Age (min)	Age of the ARP learning, in minutes
Port	Layer2 port associated with the ARP
Type	ARP type, includes the Static, Dynamic, Trust, Local.
Interface	Layer 3 interface associated with the IP addresses

Platform description	N/A

1.4.6 show arp timeout

Use this command to show the aging time of a dynamic ARP entry on the interface.

show arp timeout

Parameter description	N/A.
Command mode	Any.

Examples	The following is the output of the **show arp timeout** command:
	`DES-7200# show arp timeout`
	`Interface arp timeout(sec)`
	`---------- ----------`
	`VLAN 1 3600`
	The meaning of each field in the ARP cache table is described in Table 1.

Platform description	This command is not supported on the Layer 2 switch.

1.4.7 show ip arp

Use this command to show the Address Resolution Protocol (ARP) cache table in the privileged user mode.

show ip arp

Parameter description	N/A.
Command mode	Privileged mode.

Examples

The following is the output of **show ip arp**:

```
DES-7200# show ip arp
Protocol Address      Age(min)Hardware       Type
Interface
Internet 192.168.7.233  23   0007.e9d9.0488  ARPA
FastEthernet 0/0
Internet 192.168.7.112  10   0050.eb08.6617  ARPA
FastEthernet 0/0
Internet 192.168.7.79   12   00d0.f808.3d5c  ARPA
FastEthernet 0/0
Internet 192.168.7.1    50   00d0.f84e.1c7f  ARPA
FastEthernet 0/0
Internet 192.168.7.215  36   00d0.f80d.1090  ARPA
FastEthernet 0/0
Internet 192.168.7.127  0    0060.97bd.ebee  ARPA
FastEthernet 0/0
Internet 192.168.7.195  57   0060.97bd.ef2d  ARPA
FastEthernet 0/0
Internet 192.168.7.183  --   00d0.f8fb.108b  ARPA
FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with “-”.
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA

Interface	Interface associated with the IP address.

Platform description	This command is not supported on the Layer 2 switch.

1.4.8 show ip interface

Use this command to show the IP status information of an interface. The command format is as follows:

show ip interface [*interface-type interface-number* | **brief**]

Parameter description

Parameter	Description
interface-type	Specify interface type.
interface-number	Specify interface number.
brief	Show the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)

Command mode	Privileged mode.

Usage guidelines

When an interface is available, DES-7200 will create a direct route in the routing table. The interface is available in that the DES-7200 can receive and send packets through this interface. If the interface changes from available status to unavailable status, the DES-7200 removes the appropriate direct route from the routing table.

If the interface is unavailable, i.e. two-way communication is allowed, the line protocol status will be shown as “UP”. If only the physical line is available, the interface status will be shown as “UP”.

The results shown may vary with the interface type, because some contents are the interface-specific options.

Examples

Presented below is the output of **show ip interface brirf**:

```
DES-7200# show ip interface brief
Interface                  IP-Address(Pri)   IP-Address(Sec)
Status
GigabitEthernet 0/10  2.2.2.2/24    3.3.3.3/24        DOWN
```

```
GigabitEthernet 0/11  no address     no address        DOWN
VLAN 1                1.1.1.1/24     no address        DOWN
```

Presented below is the output of **show ip interface vlan**

```
SwitchA#show ip interface vlan 1
VLAN 1
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    1.1.1.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is:
  Proxy ARP is: OFF
  ARP packet input number:          0
     Request packet:               0
     Reply packet:                 0
     Unknown packet:               0
  TTL invalid packet number:          0
  ICMP packet input number:          0
     Echo request:                 0
     Echo reply:                   0
     Unreachable:                  0
     Source quench:                0
     Routing redirect:               0
```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface hardware status and line protocol status are “UP”.
IP interface type is:	Show the interface type, such as broadcast, point-to-point, etc.

IP interface MTU is:	Show the MTU value of the interface.
IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-boardcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachabled is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fash switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
ARP packet input number: 0 Request packet:0 Reply packet: 0 Unknown packet: 0	Show the total number of ARP packets received on the interface, including: ■ ARP request packet ■ ARP reply packet ■ Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: 0 Echo request:0 Echo reply: 0 Unreachable:0 Source quench:0 Routing redirect:0	Show the total number of ICMP packets received on the interface, including: ■ Echo request packet ■ Echo reply packet ■ Unreachable packet ■ Source quench packet ■ Routing redirection packet

Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

1.4.9 show ip packet statistics

Use this command to show the statistics of IP packets.

show ip packet statistics [total | *interface-name***]**

Parameter description

Parameter	Description
interface-name	Interface name
total	Show the total statistics of all interfaces.

Command mode

Privileged mode.

Usage guidelines

N/A

Examples

N/A

Related commands

Command	Description
-	-

2 IP Service Configuration Commands

2.1 IP Service Configuration Commands

2.1.1 ip mask-reply

Use this command to configure the DES-7200 to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. The **no** form of this command is used to prohibit from sending the ICMP mask response message.

ip mask-reply

no ip mask-reply

Default configuration	By default, no ICMP mask response message is sent.
Command mode	Interface configuration mode.
Usage guidelines	Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

Examples	The following is an example of setting the FastEthernet 0/1 interface of a device to respond the ICMP mask request message.
	`interface fastEthernet 0/1`
	`ip mask-reply`

Platform description	This command is supported on the Layer 2 switch only.

2.1.2 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. The **no** form of this command is used to restore it to the default configuration.

ip mtu *bytes*

no ip mtu

Parameter description

Parameter	Description
bytes	Maximum transmission unit of IP packet ranging 68 to 1500 bytes

Default configuration

It is the same as the value configured in the interface command **mtu** by default.

Command mode

Interface configuration mode.

Usage guidelines

If an IP packet is larger than the IP MTU, the DES-7200 will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.

If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

Examples

The following is an example of setting the IP MTU value of the fastEthernet 0/1 interface to 512 bytes.

```
interface fastEthernet 0/1
ip mtu 512
```

Related commands

Command	Description
mtu	Set the MTU value of an interface.

Platform description	This command is supported on the Layer 2 switch only.

2.1.3 ip redirects

Use this command to allow the DES-7200 to send an ICMP redirection message in the interface configuration mode. The **no** form of this command is used to disable the ICMP redirection function.

ip redirects

no ip redirects

Default configuration	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path. The DES-7200 enables ICMP redirection by default.

Examples	The following is an example of disabling ICMP redirection for the fastEthernet 0/1 interface.
	`interface fastEthernet 0/1`
	`no ip redirects`

Platform description	This command is supported on the Layer 2 switch only.

2.1.4 ip source-route

Use this command to allow the DES-7200 to process an IP packet with source route information in the global configuration mode. The **no** form of this command is used to disable the source route information processing function.

ip source-route

no ip source-route

Default configuration	Enabled.
Command mode	Global configuration mode.
Usage guidelines	DES-7200 supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded. The DES-7200 supports IP source route by default.
Examples	The following is an example of disabling the IP source route. `no ip source-route`
Platform description	This command is supported on the Layer 2 switch only.

2.1.5 ip unreachables

Use this command to allow the DES-7200 to generate ICMP destination unreachable messages. The **no** form of this command disables this function.

ip unreachables

no ip unreachables

Default configuration	Enabled.

Command mode	Interface configuration mode.
Usage guidelines	DES-7200 will send an ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upeer protocol of this message. DES-7200 will send ICMP host unreachable message to source data if it can not forward a message due to no routing. This command influences all ICMP destination unreachable messages.
Examples	The following example disables sending ICMP destination unreachable message on FastEthernet 0/1. **interface fastEthernet** *0/1* **no ip unreachables**
Platform description	This command is not supported on the Layer 2 switch.

3 IPv6 Configuration Commands

3.1 Configuration Related Commands

3.1.1 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to delete the configured address.

ipv6 address ipv6-address/prefix-length

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

ipv6 address *prefix-name sub-bits/prefix-length* **[eui-64]**

no ipv6 address

no ipv6 address *ipv6-address/prefix-length*

no ipv6 address *ipv6-prefix/prefix-length* **eui-64**

no ipv6 address *prefix-name sub-bits/prefix-length* **[eui-64]**

	Parameter	Description
Parameter description	*ipv6-prefix*	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	ipv6-address	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.

prefix-length	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of DES-7200 is 0 to 64 or 128 to 128.
prefix-name	The general prefix name.Use the specified general prefix to generate the interface address.
sub-bits	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
eui-64	The generated IPV6 address consists of the address prefix and the 64 bit interface ID.

Command mode

Interface configuration mode

Usage guidelines

When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.

The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.

If no deleted address is specified when using **no ipv6 address**, all the manually configured addresses will be deleted.

no ipv6 address *ipv6-prefix***/***prefix-length* **eui-64** can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix***/***prefix-length* **eui-64**.

	 **Caution** For the DES-7200 series, The length of the IPv6 address prefix is not limited, but there are 512 IPv6 routings of which prefix length supported by the switch is in the range of 65 to 127.

Examples	DES-7200(config-if)# **ipv6 address** *2001:1::1/64* DES-7200(config-if)# **no ipv6 address** *2001:1::1/64* DES-7200(config-if)# **ipv6 address** *2002:1::1/64 eui-64* DES-7200(config-if)# **no ipv6 address** *2002:1::1/64 eui-64*

3.1.2 ipv6 address autoconfig

Use this command to automatically configure an IPv6 stateless address for a network interface. Use the **no** form of this command to delete the auto-configured address.

ipv6 address autoconfig[**default**]

no ipv6 address autoconfig

	Parameter	Description
Parameter description	**default**	(Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the **default** keyword.

Command mode	Interface configuration mode

Usage guidelines	The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address. If the RA message contains the flag of the “other configurations”, the interface will obtain these “other configurations” through the DHCPv6. The “other configurations” usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc. Use the **no ipv6 address autoconfig** command to delete the IPv6 address.

Examples	`DES-7200(config-if)# ipv6 address autoconfig default` `DES-7200(config-if)# no ipv6 address autoconfig`

Related commands	**Command**	**Description**
	ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]	Configure the IPv6 address for the interface manually .

3.1.3 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to disable this function.

ipv6 enable

no ipv6 enable

Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.

Caution

If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.

Examples	`DES-7200(config-if)# ipv6 enable`

Related commands	**Command**	**Description**
	show ipv6 interface	Show the related information of an interface.

3.1.4 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

no ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

Parameter description

Parameter	Description
prefix-name	The general prefix name.
pv6-prefix	The network prefix value of the general-prefix following the format defined in RFC4291.
prefix-length	The length of the general prefix.

Command mode

Global configuration mode.

Usage guidelines

It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.

A general prefix could contain multiple prefixes.

These longer specified prefixes is usually used for the Ipv6 address configuration on the interface.

Examples

The following example configures manually a general prefix as my-prefix.

```
DES-7200(config)# ipv6 general-prefix my-prefix
2001:1111:2222::/48
```

Related commands

Command	Description
ipv6 address prefix-name sub-bits/prefix-length	Configure the interface address using the general prefix.
show ipv6 general-prefix	Show the general prefix.

3.1.5 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

ipv6 hop-limit *value*

no ipv6 hop-limit

Default configuration	The default is 64.
Command mode	Global configuration mode.
Usage guidelines	This command takes effect for the unicast messages only, not for multicast messages.
Examples	DES-7200(config)# **ipv6 hop-limit** *100*

3.1.6 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to remove the setting.

ipv6 neighbor *ipv6-address interface-id hardware-address*

no ipv6 neighbor ipv6-address interface-id

Parameter description

Parameter	Description
ipv6-address	IPv6 address of the neighbor. It must follow the address format defined in RFC4291.
interface-id	Network interface of the neighbor (including routed Port, L3 AP interface, or SVI interface).
hardware-address	Hardware address of the neighbor. It shall be a 48-bit MAC address in the format of XXXX.XXXX.XXXX, where “X” is a hexadecimal number.

Default configuration	No static neighbor is configured.

Command mode	Global configuration mode.
Usage guidelines	Similar to the ARP command, the static neighbor can only be configured on an IPv6 protocol enabled interface. If the neighbor to be configured has been learned through NDP and has been stored in the neighbor list, the dynamically generated neighbor will be automatically switched to a static one. The configured static neighbor is always in the **Reachable** status. Use **clear ipv6 neighbors** to clear all the neighbors dynamically learned through NDP. Use **show ipv6 neighbors** to view the neighbor information.
Examples	`DES-7200(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111`

Related commands

Command	Description
show ipv6 neighbors	Show the neighbor information.
clear ipv6 neighbors	Clear the neighbors learned dynamically.

3.1.7 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts

Parameter description

Parameter	Description
value	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

Default configuration	1.

Command mode	Interface configuration mode.
Usage guidelines	When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the ”tentative” status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.
Examples	`DES-7200(config-if)# ipv6 nd dad attempts 3`

Related commands

Command	Description
show ipv6 interface	Show the interface information.

3.1.8 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to remove the setting.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Default configuration	None.
Command mode	Interface configuration mode.
Usage guidelines	This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP

	address through stateful auto configuration, otherwise it does not be used.

Examples

```
DES-7200(config-if)# ipv6 nd managed-config-flag
```

Related commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd other-config-flag	Set the flag for obtaining all information except IP address through stateful auto configuration.

3.1.9 ipv6 nd other-config-flag

Use this command to set “other stateful configuration” flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameter description

Parameter	Description
-	-

Default configuration

The flag bit is not set by default.

Command mode

Interface configuration mode.

Usage guidelines

With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set.

Examples

```
DES-7200(config-if)# ipv6 nd other-config-flag
```

Related

Command	Description

	show ipv6 interface	Show the interface information**.**

3.1.10 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore it to the default setting.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Parameter description	**Parameter**	**Description**
	milliseconds	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds

Default configuration	The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000ms(1s).
Command mode	Interface configuration mode.
Usage guidelines	The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.
Examples	`DES-7200(conifig-if)# ipv6 nd ns-interval 2000`

Related commands	**Command**	**Description**
	show ipv6 interface	Show the interface information**.**

3.1.11 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore it to the default setting.

ipv6 nd prefix {*ipv6-prefix*/*prefix-length* | **default** }[[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | [**infinite** | *preferred-lifetime*]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]

no ipv6 nd prefix {*ipv6-prefix/prefix-length* | **default** }[[**off-link**] [**no-autoconfig**] | [**no-advertise**]]

Parameter description

Parameter	Description
ipv6-prefix	IPv6 network ID following the format defined in RFC4291
prefix-length	Length of the IPv6 prefix. "/" shall be added in front of the prefix
valid-lifetime	Valid lifetime of the RA prefix received by the host
preferred-lifetime	Preferred lifetime of the RA prefix received by the host
at *valid-date preferred-date*	Set the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
infinite	Indicate that the prefix is always valid.
default	Set the default perfix.
no-advertise	The prefix will not be advertised by the device.
off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
no-autoconfig	Indicate that the RA prefix received by the host cannot be used for auto address configuration.

Default configuration

By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:

valid-lifetime: 2592000s (30 days)

preferred-lifetime: 604800s (7 days),

The prefix is advertised and is used for on-link judgment and auto address configuration.

Command mode

Interface configuration mode.

Usage

This command can be used to configure the parameters of

guidelines

each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

ipv6 nd prefix default

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

at *valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

Examples

The following example adds a prefix for SVI 1.

```
DES-7200(config)# interface vlan 1
DES-7200(conifig-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 prefix default no-autoconfig
```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related commands

Command	Description
show ipv6 interface	Show the RA information of an interface.

3.1.12 ipv6 nd ra-hoplimit

Use this command to set the hopcount of the RA message. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-hoplimit *value*

no ipv6 nd ra-hoplimit

Parameter description

Parameter	Description
value	Hopcount

Default configuration

The default value is 64.

Command mode

Interface configuration mode.

Usage guidelines

It is used to set the hopcount of the RA message.

Examples

```
DES-7200(config -if)# ipv6 nd ra-hoplimit 110
```

Related commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd ra-lifetime	Set the lifetime of the device.
ipv6 nd ra-interval	Set the interval of sending the RA message.
ipv6 nd ra-mtu	Set the MTU of the RA message.

3.1.13 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-interval {*seconds* | **min-max** *min_value max_value*}

no ipv6 nd ra-interval

Parameter description

Parameter	Description
seconds	Interval of sending the RA message in seconds, 3-1800s.
min-max	Maximum and minimum interval sending the RA message in seconds
min_value	Minimum interval sending the RA message in seconds

	max_value	Maximum interval sending the RA message in seconds

Default configuration	200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.
Command mode	Interface configuration mode.
Usage guidelines	If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value. If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.
Examples	`DES-7200(conifig-if)# ipv6 nd ra-interval 110` `DES-7200(config-if)# ipv6 nd ra-interval min-max 110 120`

Related commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd ra-lifetime	Set the lifetime of the device.
ipv6 nd ra-hoplimit	Set the hopfcount of the RA message.
ipv6 nd ra-mtu	Set the MTU of the RA message.

3.1.14 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameter description

Parameter	Description
seconds	Default life time of the device on the interface, 0-9000.

Default configuration 1800s.

Command mode Interface configuration mode.

Usage guidelines The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval).

Examples

```
DES-7200(conifig-if)# ipv6 nd ra-lifetime 2000
```

Related commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd ra-interval	Set the interval of sending the RA.
ipv6 nd ra-hoplimit	Set the hopcount of the RA.
ipv6 nd ra-mtu	Set the MTU of the RA.

3.1.15 ipv6 nd ra-mtu

Use this command to set the MTU of the RA messag. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-mtu *value*

no ipv6 nd ra-mtu

Parameter description

Parameter	Description
value	MTU value, 0-4294967295.

Default configuration IPv6 MTU value of the network interface.

Command mode	Interface configuration mode.
Usage guidelines	If it is specified as 0, the RA will not have the MTU option.
Examples	`DES-7200(config -if)# ipv6 nd ra-mtu 1400`

Related commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd ra-lifetime	Set the lifetime of the device.
ipv6 nd ra-interval	Set the interval of sending the RA message.
ipv6 nd ra-hoplimit	Set the hopcount of the RA message.

3.1.16 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore it to the default setting.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Parameter description

Parameter	Description
milliseconds	Reachable time for the neighbor in the range 0 to 3600000 milliseconds.

Default configuration	The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000ms(30s) when the device discovers the neighbor.
Command mode	Interface configuration mode.
Usage guidelines	The device checks the unreachable neighbor through the set time. A shorter time means that the device can check

	the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time. The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used. According to RFC4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5*configured value to 1.5*configured value.

Examples

```
DES-7200(config-if)# ipv6 nd reachable-time 1000000
```

Related commands

Command	Description
show ipv6 interface	Show the interface information.

3.1.17 ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message. Use the **no** form of this command to enable the function.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Default configuration	The RA message is not sent on the IPv6 interface by default.
Command mode	Interface configuration mode.
Usage guidelines	This command suppresses the sending of the RA message on an interface.

Examples

```
DES-7200(config-if)# ipv6 nd suppress-ra
```

Related commands

Command	Description
show ipv6 interface	Show the interface information.

3.1.18 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. When **no ipv6 ns-linklocal-src** is executed, the global IP address will be taken as the source address to send neighbor requests.

ipv6 ns-linklocal-src

no ipv6 ns-linklocal-src

Default configuration	The local address of the link is always used as the source address to send neighbor requests.
Command mode	Global configuration mode.
Usage guidelines	None.
Examples	`DES-7200(config)# no ipv6 ns-linklocal-src`

3.1.19 ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to disable the function.

ipv6 redirects

no ipv6 redirects

Default configuration	The ICMPv6 redirect message is permitted to be sent on the IPV6 interface.
Command mode	Interface configuration mode.
Usage guidelines	The transmission rate of any ICMPv6 error message is limited. By default, it is 10pps.
Examples	`DES-7200(config-if)# ipv6 redirects`

Related	**Command**	**Description**

	show ipv6 interface	Show the interface information.

3.1.20 ipv6 route

Use this command to configure an IPv6 static route. Use the **no** form of this command to remove the setting.

ipv6 route *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-id* [*ipv6-address*] } [*distance*] [**weight** *number*]

	Parameter	Description
Parameter description	*ipv6-prefix*	IPV6 network number following the format specified in RFC4291. prefix-length: Length of the IPv6 prefix. "/" must be added in front of the prefix. Note: The prefix length range of the static routes of DES-7200 is 0 to 64 or 128 to 128.
	ipv6-address	Next-hop IP address to the destination address. It shall be in the format defined in RFC4291. The next-hop IP address and the next-hop outgoing interface can be specified at the same time. Note that if the next-hop IP address is a link-local address, the outgoing interface must be specified.
	vrf-name1	VRF in the nexthop, which must be the multi-protocol VRF with the IPv6 address family configured.
	interface-id	The outgoing interface toward the destination network. If the static route is configured with the outgoing interface but no next-hop address is specified, the destination address will be considered on the link connected with the outgoing interface; that is to say, the static route will be treated as a directly-connected route. Note that if the destination network or next-hop address is a link-local address, the outgoing interface must be specified.

Command mode	Global configuration mode.
Usage guidelines	Note: If the destination IP address or next-hop IP address is a link-local IP address, the outgoing interface must be specified; if the destination address is a link-local IP address, the next-hop must be also a link-local IP address. When configuring a route, the destination IP address and the next-hop IP address shall not be a multicast address. If both the next hop IP address and the outgoing interface are specified, the outgoing interface of the direct route that matches the next hop shall be the same as the configured outgoing interface.
Examples	`DES-7200(config)# ipv6 route 2001::/64 vlan 1 2005::1`
Platform description	None

Related commands

Command	Description
show ipv6 route	Show the IPv6 route information.

3.1.21 ipv6 source-route

Use this command to forward the IPv6 packet with route header. The **no** form of this command disables the forwarding.

ipv6 source-route

no ipv6 source-route

Parameter description	None.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage	Because of the potential security of the header of type 0

guidelines	route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.
Examples	`DES-7200(config)# no ipv6 source-route`
Related commands	None.

3.1.22 ping ipv6

Use this command to diagnose the connectivity of the IPv6 network.

ping ipv6 [*ipv6-address*]

Parameter description

Parameter	Description
ipv6-address	Destination IP address to be diagnosed.

Command mode

Privileged mode.

Usage guidelines

If no destination address is entered in the command, the user interaction mode is entered, and you can specify the parameters. The following table shows the meanings of symbols returned by the **ping** command:

Signs	Meaning
!	The response to each request sent is received.
.	The response to the request sent is not received within a regulated time.
U	The device has no route to the destination host.
R	Parameter error.
F	No system resource is available.
A	The source IP address of the packet is not selected.

D	The network interface is in the **Down** status, or the IPv6 function is disabled on the the interface (for example, IP address collision is detected).
?	Unknown error

Examples

```
DES-7200# ping ipv6 fec0::1
```

3.2 Showing Related Command

3.2.1 clear ipv6 neighbors

Use this command to clear the dynamically learned neighbors.

clrear ipv6 neighbors

Parameter description

Parameter	Description
vrf-name	VRF name

Command mode

Privileged mode.

Usage guidelines

This command can be used to clear all the neighbors dynamically learned by the neighbor discovering. Note that the static neighbors will not be cleared.

Examples

```
DES-7200# clear ipv6 neighbors
```

Related commands

Command	Description
ipv6 neighbor	Configure the neighbor.
show ipv6 neighbors	Show the neighbor information.

Platform description

N/A

3.2.2 show ipv6 address

Use this command to show the IPv6 addresses.

show ipv6 address [*interface-name***]**

Parameter description

Parameter	Description
interface-name	Interface name

Command mode

Privileged mode.

Usage guidelines

N/A

Examples

N/A

Platform description

N/A

3.2.3 show ipv6 general-prefix

Use this command to show the information of the general prefix.

show ipv6 general-prefix

Command mode

Privileged mode.

Usage guidelines

Use this command to show the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

Examples

The following example shows the information of the general prefix

```
DES-7200# show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix my-prefix, acquired via Manual
configuration
       2001:1111:2222::/48
       2001:1111:3333::/48
```

Related

Command	Description

	ipv6 general-prefix	Configure the general prefix.

3.2.4 show ipv6 interface

Use this command to show the IPv6 interface information.

show ipv6 interface [*interface-id*] [**ra-info**]

	Parameter	Description
Parameter description	*interface-id*	Interface (including Ethernet interface, aggregateport, or SVI)
	ra-info	Show the RA information of the interface.

Command mode	Privileged mode.
Usage guidelines	Use this command to show the address configuration, ND configuration and other information of an IPv6 interface.

Examples

```
DES-7200# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
```

```
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds
```

The following line is included in the above information: 2001::1, subnet is 2001::/64 [**TENTATIVE**]. The flag bit in the [ ] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.

```
DES-7200# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags:
LA)
```

Description of the fields in **ra-info**:

Field	Meaning
RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.

initcount	Indicate the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M | M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O | O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	Meaning
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicate that the interfaces use the default prefix.
Auto | CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.
vltime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.

L | !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A | !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

3.2.5 show ipv6 neighbors

Use this command to show the IPv6 neighbors.

show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]

show ipv6 neighbors static

Parameter description

Parameter	Description
verbose	Show the neighbor details.
static	Show the validity status of static neighbors.
interface-id	Show the neighbors of the specified interface.
ipv6-addres	Show the neighbors of the specified IPv6 address.

Command mode

Privileged mode.

Usage guidelines

Show the neighbors on the SVI 1 interface:

```
DES-7200# show ipv6 neighbors vlan 1
IPv6 Address Linklayer Addr   Interface
fa::1         00d0.0000.0002   vlan 1
fe80::200:ff:fe00:2  00d0.0000.0002  vlan 1
```

Show the neighbor details:

```
DES-7200# show ipv6 neighbors verbose
IPv6 Address  Linklayer Addr Interface
2001::1      00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1    00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
```

Field	Meaning
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, **incomplete** is displayed.

Interface	Interface the neighbor locates.
State	State of the neighbor: state/H(R) The values of **STATE** are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3). ?: Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.
Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.

	Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

Examples

```
DES-7200# show ipv6 neighbors
```

Related commands

Command	Description
ipv6 neighbor	Configure a neighbor.

3.2.6 show ipv6 neighbors statistics

Use the following command to show the statistics of one IPv6 neighbors.

show ipv6 neighbors statistics

Use the following command to show the statistics of all IPv6 neighbors.

show ipv6 neighbors statistics all

Parameter description

Parameter	Description
-	-

Command mode

Privileged mode.

Examples

N/A

Related commands

Command	Description
-	-

Platform description

Supported on all platforms.

3.2.7 show ipv6 packet statistics

Use this command to show the statistics of IPv6 packets.

show ipv6 packet statistics [total | *interface-name***]**

Parameter description

Parameter	Description
total	Show total statistics of all interfaces.
interface-name	Interface name

Command mode

Privileged mode.

Usage guidelines

N/A

Examples

N/A

Related commands

Command	Description
-	-

Platform description

Supported on all platforms.

3.2.8 show ipv6 route

Use this command to show the IPv6 route information.

show ipv6 route [**static** | **local** | **connected**]

Parameter description

Parameter	Description
static	Show the static routes.
local	Show the local routes.
connected	Show the directly-connected routes.

Command mode

Privileged mode.

Usage guidelines

Use this command to view the routing table.

Examples

```
DES-7200# show ipv6 route
Codes: C - Connected, L - Local, S - Static, R - RIP, B
```

```
- BGP
      I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
L    ::1/128
     via ::1, loopback 0
C    fa::/64
     via ::, vlan 1
L    fa::1/128
     via ::, loopback 0
C    2001::/64
     via ::, vlan 2
L    2001::1/128
     via ::, loopback 0
L    fe80::/10
     via ::1, Null0
C    fe80::/64
     via ::, vlan 1
L    fe80::200:ff:fe00:1/128
     via ::, loopback 0
C    fe80::/64
     via ::, vlan 2
```

Related commands

Command	Description
ipv6 route	Configure a static route.

Platform description N/A

3.2.9 show ipv6 route summary

Use the following command to show the statistics of one IPv6 route table.

show ipv6 route summary

Use the following command to show the statistics of all IPv6 route tables.

show ipv6 route summary all

Parameter description

Parameter	Description
-	-

Command mode Privileged mode.

Usage N/A

guidelines	
Examples	N/A

Related commands	**Command**	**Description**
	ipv6 route	Configure a static route.

Platform description	N/A

3.2.10 show ipv6 routers

In the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to show the neighbor routers and the advertisement.

show ipv6 routers *[interface-type interface-number]*

Parameter description	**Parameter**	**Description**
	interface-type interface-number	(Optional) Show the routing advertisement of the specified interface.

Command mode	Privileged mode.
Usage guidelines	Use this command to show the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.

Examples	The following example shows the IPv6 router
	`DES-7200# show ipv6 routers`
	`Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec`
	`  Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500`
	`  Preference=MEDIUM`
	`  Reachable time 0 msec, Retransmit time 0 msec`
	`  Prefix 6001:3::/64 onlink autoconfig`
	`    Valid lifetime 2592000 sec, preferred lifetime 604800 sec`

```
  Prefix 6001:2::/64 onlink autoconfig
    Valid lifetime 2592000 sec, preferred lifetime 604800
sec
```

4 IPv6 Tunnel Configuration Commands

4.1 Configuration Related Commands

4.1.1 tunnel destination

Use this command to specify the destination address for the tunnel. Use the **no** form of this command to remove the setting.

tunnel destination {*ipv4-address* **}**

no tunnel destination

Parameter description

Parameter	Description
ipv4-address	Destination address of the tunnel, namely the IPv4 address in the other side of the tunnle..

Default configuration

The destination address encapsulated by the tunnel is not configured by default.

Command mode

Interface configuration mode.

Usage guidelines

A device shall not be configured multiple tunnels with the same encapsulation type, source address and destination address.

Note: For auto tunnel (isatap), the destination address shall not be configured.

Examples

The following example configures an IPv6 manual tunnel.

```
DES-7200(config)# interface tunnel 1
DES-7200(config-if)# tunnel mode ipv6ip
DES-7200(config-if)# tunnel source vlan 1
DES-7200(config-if)# tunnel destination 192.168.5.1
```

Related commands

Command	Description
tunnel source	Configure the source IP address of the tunnel.
tunnel mode	Configure the mode of a tunnel.

4.1.2 tunnel mode ipv6ip

Use this command to configure static IPv6 tunnel mode. Use the **no** form of this command to restore it to the default IPv6 tunnel mode.

tunnel mode ipv6ip [isatap]

no tunnel mode

Parameter description

Parameter	Description
isatap	Configure the tunnel as an auto ISATAP tunnel.

Default configuration

The type of the configured IPv6 tunnel is a tunnel configured manually.

Command mode

Interface configuration mode.

Usage guidelines

After a tunnel is created, it is considered to be manual tunnel by default. You can also use **tunnel mode ipv6ip** without any parameter to set a tunnel to manual tunnel. For an auto tunnel, no destination address is specified.

Examples

The following example configures an ISATAP tunnel.

```
DES-7200(config)# interface tunnel 1
DES-7200(config-if)# tunnel mode ipv6ip isatap
DES-7200(config-if)# tunnel source vlan 1
```

Related commands

Command	Description
tunnel source	Configure the source address of the tunnel.
tunnel destination	Configure the destination address of a tunnel.

4.1.3 tunnel source

Use this command to specify the source IP address for the tunnel. Use the **no** form of this command to remove the setting.

tunnel source {*ipv4-address* | *interface-type interface-number*}

no tunnel source

Parameter description

Parameter	Description
ipv4-address	Source IPv4 address of the tunnel used as the source IP address of the packets to be transmitted through the tunnel.
interface-type interface-number	Interface referenced by the tunnel, which will be used as the source IPv4 address of the packets to be transmitted through the tunnel.

Default configuration

No tunnel source address is configured by default.

Command mode

Interface configuration mode.

Usage guidelines

The source IP address of a tunnel can be a specified IPv4 address or an IPv4 address of an interface.

Examples

The following example configures an IPv6 manual tunnel.

```
DES-7200(config)# interface tunnel 1
DES-7200(config-if)# tunnel mode ipv6ip
DES-7200(config-if)# tunnel source vlan 1
DES-7200(config-if)# tunnel destination 192.168.5.1
```

Related commands

Command	Description
tunnel mode	Configure the mode of a tunnel.
tunnel destination	Configure the destination address of a tunnel.

5 DHCP Configuration Commands

5.1 DHCP Configuration Related Command

5.1.1 address range

Use this command to specify the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool.The **no** form of this command can be used to remove the network segment range.

address range *low-ip-address high-ip-address*

no address range

Parameter description

Parameter	Description
low-ip-address	Start address in the network segment range.
high-ip-address	End adress in the network segment range.

Default

By default, the associated CLASS is not configured the network segment range. It is defaulted to the address pool range.

Command mode

Address pool CLASS configuration mode.

Usage guidelines

Each CLASS corresponds to one network range which must be from low address to high address, so as to allow the duplication of network segment range between multiple CLASSs. If the CLASS associated with the address pool is specified without configuring the corresponding network segment range, the default network segment range of this CLASS is same as the range of the address pool where this CLASS is.

Examples

The configuration example below configures the network segment of class1 associated with address pool mypool0 ranging from 172.16.1.1 to 172.16.1.8.

```
DES-7200(config)# ip dhcp pool mypool0
DES-7200(dhcp-config)# class class1
DES-7200 (config-dhcp-pool-class)# address range 172.16.1.1 172.16.1.8
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.
class	Configure the CLASS associated with the DHCP address pool and enter into the address pool CLASS configuration mode.

5.1.2 bootfile

Use this command to define the startup mapping file name of the DHCP client in the DHCP address pool configuration mode.The **no** form of this command can be used to remove the definition.

bootfile file-name

no bootfile

Parameter description

Parameter	Description
file-name	Startup file name.

Default

No startup file name is defined, by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

Examples

The configuration example below defines the device.conf as the startup file name.

```
bootfile device.conf
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.
next-server	Configure the next server IP address of the DHCP client startup process.

5.1.3 class

Use this command to configure the associted CLASS in the DHCP address pool.The **no** form of this command is used to delete the associated CLASS.

class *class-name*

no class

Parameter description

Parameter	Description
class-name	Class name, which can be the character string or numeric such as myclass or 1.

Default

By default, no CLASS is associated with the address pool.

Command mode

DHCP address pool configuration mode.

Usage guidelines	Each DHCP address pool performs the address assignment according to the Option82 matching information. We can divide this Option82 information into classes and specify the available network segment range for these classes in the DHCP address pool. These classes are called CLASS. One DHCP address pool can map to multiple CLASSes, and each CLASS can specify different network segment range. During the address assignment, firstly, ensure the assignable address pool through the network segment where the client is, then according to the Option82 information further ensure the CLASS and assign the IP address from the network segment range corresponding to the CLASS. If one request packet matches multiple CLASSes in the address pool, perform the address assignment according to the sequencing of configuring the CLASS in the address pool. If this CLASS's assigned addresses have been to the upper limit, then continue to assign the address from the next CLASS, and so on. Each CLASS corresponds to one network segment range that must be from low addresses to high addresses and the duplicated network ranges between multiple CLASSes are allowed. If the CLASS corresponding to the address pool is specified, this CLASS's default network segment range is same as the range of address pool where the CLASS is.

Examples	The configuration example below configures the address *mypool0* to associate with class1.
	`DES-7200(config)# ip dhcp pool mypool0`
	`DES-7200(dhcp-config)# class class1`

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.4 client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the client ID.

client-identifier *unique-identifier*

no client-identifier

Parameter description

Parameter	Description
unique-identifier	The DHCP client ID, indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

Default N/A.

Command mode DHCP address pool configuration mode.

Usage guidelines

When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather then their hardware addresses. The client ID consists of media type, MAC address and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media.

The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/1. For the definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700.

This command is used only when the DHCP is defined by manual binding.

Examples

The configuration example below defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```
client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

Related commands

Command	Description
hardware-address	Define the hardware address of DHCP client.
host	Define the IP address and network mask, which is used to configure the DHCP manual binding.

	ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.5 client-name

Use this command to define the name of the DHCP client in the DHPC address pool configuration mode.The **no** form of this command is used to delete the name of the DHCP client.

client-name *client-name*

no client-name

Parameter description	**Parameter**	**Description**
	client-name	Name of DHCP client, a set of standards-based ASCII characters.The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn.

Default	No client name is defined.
Command mode	DHCP address pool configuration mode.
Usage guidelines	This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.
Examples	The configuration example below defines a string river as the name of the client. `client-name river`

Related commands	**Command**	**Description**
	host	Define the IP address and network mask, which is used to configure the DHCP manual binding.

	ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.6 default-router

Use this command to define the default gateway of the DHCP client in the DHPC address pool configuration mode.The **no** form of this command can be used to delete the definition of the default gateway.

default-router *ip-address* [*ip-address2…ip-address8*]

no default-router

Parameter description

Parameter	Description
ip-address	Define the IP address of the equipment. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) Up to 8 gateways can be configured.

Default No gateway is defined by default.

Command mode DHCP address pool configuration mode.

Usage guidelines In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.

Examples The configuration example below defines 192.168.12.1 as the default gateway.

```
default-router 192.168.12.1
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.7 dns-server

Use this command to define the DNS server of the DHCP client in the DHPC address pool configuration mode. The **no** form of this command can be used to delete the definition of the DNS server.

dns-server { *ip-address* [*ip-address2…ip-address8*] | **use-dhcp-client** *interface-type interface-number* }

no dns-server

Parameter description

Parameter	Description
ip-address	Define the IP address of the DNS server. At least one IP address should be configured.
ip-address2…ip-address8	(Optional) Up to 8 DNS servers can be configured.
use-dhcp-client *interface-type interface-number*	Use the DNS server learned by the DHCP client of the DES-7200 as the DNS server of the DHCP client.

Default

No DNS server is defined by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

When more than one DNS server is defined, the former will possess higher priory, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails.

If the DES-7200 also acts as the DHCP client, the DNS server information obtained by the client can be transmitted to the DHCP client.

Examples

The configuration example below specifies the DNS server 192.168.12.3 for the DHCP client.

```
dns-server 192.168.12.3
```

Related commands

Command	Description
domain-name	Define the suffix domain name of the DHCP client.

ip address dhcp	Enable the DHCP client on the interface to obtain the IP address information.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.8 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHPC address pool configuration mode. The **no** form of this command can be used to delete the suffix domain name.

domain-name *domain-name*

no domain-name

Parameter description

Parameter	Description
domain-name	Define the suffix domain name string of the DHCP client.

Default No suffix domain name by default.

Command mode DHCP address pool configuration mode.

Usage guidelines After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.

Examples The configuration example below defines the suffix domain name i-net.com.cn for the DHCP client.

```
domain-name i-net.com.cn
```

Related commands

Command	Description
dns-server	Define the DNS server of the DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.9 hardware-address

Use this command to define the hardware address of the DHCP client in the DHPC address pool configuration mode.The **no** form of this command can be used to delete the definition of the hardware address.

hardware-address *hardware-address [type]*

no hardware-address

Parameter description

Parameter	Description
hardware-address	Define the MAC address of the DHCP client.
type	To indicate the hardware platform protocol of the DHCP client, use the string definition or digits definition. String option: ■ Ethernet ■ ieee802 Digits option: ■ 1 (10M Ethernet) ■ 6 (IEEE 802)

Default

No hardware address is defined by default.

If there is no option when the hardware address is defined, it is the Ethernet by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

This command can be used only when the DHCP is defined by manual binding.

Examples

The configuration example below defines the MAC address 00d0.f838.bf3d with the type ethernet.

```
hardware-address 00d0.f838.bf3d
```

Related commands

Command	Description
client-identifier	Define the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot).

host	Define the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.10 host

Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the definition of the IP address and network mask for the DHCP client.

host *ip-address* [*netmask*]

no host

Parameter description

Parameter	Description
ip-address	Define the IP address of DHCP client.
netmask	Define the network mask of DHCP client.

Default No IP address or network mask of the host is defined.

Command mode DHCP address pool configuration mode.

Usage guidelines

If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address.

This command can be used only when the DHCP is defined by manual binding.

Examples

The configuration example below sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240.

```
host 192.168.12.91 255.255.255.240
```

Related commands	Command	Description
	client-identifier	Define the unique ID of the DHCP client (Indicated in hex, separated by dot).
	hardware-address	Define the hardware address of DHCP client.
	ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.11 ip address dhcp

Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. The **no** form of this command can be used to cancel this configuration.

ip address dhcp

no ip address dhcp

Default	The interface cannot obtain the ID address by the DHCP by default.
Command mode	Interface configuration mode.
Usage guidelines	When requesting the IP address, the DHCP client of the DES-7200 also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information. The client of the DES-7200 is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server. At present, our server can support this function.
Examples	The configuration example below makes the FastEthernet 0 port obtain the IP address automatically.

```
interface fastEthernet 0
ip address dhcp
```

Related commands

Command	Description
dns-server	Define the DNS server of DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.12 ip dhcp class

Use this command to define a CLASS and enter the global CLASS configuration mode. The **no** form of this command can be used to delete the global CLASS.

ip dhcp class *class-name*

no ip dhcp class *class-name*

Parameter description

Parameter	Description
class-name	Class name, which can be character string or numeric such as myclass or 1.

Default By default, the class is not configured.

Command mode Global configuration mode.

Usage guidelines After executing this command, it enters the global CLASS configuration mode which is shown as "`DES-7200(config-dhcp-class)#`". In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.

Examples The configuration example below configures a global CLASS.

`DES-7200(config)#` **`ip dhcp class`** *`myclass`*

Related commands

Command	Description
-	-

5.1.13 ip dhcp database write-delay

Use this command to configure the function of writing the DHCP lease data-binding information into the FLASH timely in the global configuration mode. The **no** form of this command can be used to disable the function of writing timely.

ip dhcp database write-delay *time*

no ip dhcp database write-delay

Parameter description

Parameter	Description
time	The interval at which the system writes the DHCP lease binding database information into the flash.

Default Disabled

Command mode Global configuration mode.

Usage guidelines By configuring this command, you can write the information of DHCP lease binding database into the FLASH files to prevent the loss of user information after restarting the device.

Examples The configuration example below sets the interval at which the switch writes the information into FLASH as 3600s.

```
DES-7200(config)# ip dhcp database write-delay 3600
```

Related commands

Command	Description
-	-

5.1.14 ip dhcp database write-to-flash

Use this command to write the information of DHCP lease binding data into FLASH files in the real-time..

ip dhcp database write-to-flash

Parameter description

Parameter	Description
-	-

Default	N/A
Command mode	Global configuration mode.
Usage guidelines	By configuring this command, you can write the information of DHCP lease binding database into the FLASH files in real-time.
Examples	The configuration example below writes the binding database information into FLASH manually. `DES-7200(config)# ip dhcp database write-to-flash`

Related commands

Command	Description
-	-

5.1.15 ip dhcp excluded-address

Use this command to define some IP addresses and make the DHCP server not assign them to the DHCP client in the global configuration mode. The **no** form of this command can be used to cancel this definition.

ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

no ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

Parameter description

Parameter	Description
low-ip-address	Exclude the IP address, or exclude the start IP address within the range of the IP address.
high-ip-address	Exclude the end IP address within the range of the IP address.

Default	The DHCP server assigns the IP addresses of the whole address pool by default.
Command mode	Global configuration mode.

Usage guidelines	If the excluded IP address is not configured, the DHCP server attempts to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts to prevent these addresses are assigned to the DHCP client, and define the excluded IP address accurately to reduce the conflict detecting time when the DHCP server assigns the address.
Examples	In the configuration example below, the DHCP server will not attempt to assign the IP addresses within 192.168.12.100~150. `ip dhcp excluded-address 192.168.12.100 192.168.12.150`

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.
network (DHCP)	Define the network number and network mask of the DHCP address pool.

5.1.16 ip dhcp ping packet

Use this command to configure the times of pinging the IP address when the DHCP server detects address conflict in the global configuration mode. The **no** form of this command is used to restore it to the default configuration.

ip dhcp ping packet [*number*]

no ip dhcp ping packet

Parameter description

Parameter	Description
number	(Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default.

Default	The Ping operation sends two packets by default.
Command mode	Global configuration mode.

Usage guidelines	When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.
Examples	The configuration example below sets the number of the packets sent by the ping operation as 3. `ip dhcp ping packets 3`

Related commands

Command	Description
clear ip dhcp conflict	Clear the DHCP history conflict record.
ip dhcp ping packet	Configure the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned. Otherwise, it will record the address conflict.
show ip dhcp conflict	Show the DHCP server detects address conflict when it assigns an IP address.

5.1.17 ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. The **no** form of this command can be used to restore it to the default configuration.

ip dhcp ping timeout *milli-seconds*

no ip dhcp ping timeout

Parameter description

Parameter	Description
milli-seconds	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

Default	The default timeout is 500 seconds.

Command mode	Global configuration mode.
Usage guidelines	This command defines the time that the DHCP server waits for a ping response packet.
Examples	In the configuration example below, the waiting time of the ping response packet is 600ms. `ip dhcp ping timeout 600`

Related commands

Command	Description
clear ip dhcp conflict	Clear the DHCP history conflict record.
ip dhcp ping packets	Define the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
show ip dhcp conflict	Show the address conflict the DHCP server detects when it assigns an IP address.

5.1.18 ip dhcp pool

Use this command to define a name of the DHCP address pool and enter into the DHCP address pool configuration mode in the global configuration mode.The **no** form of this command can be used to delete the DHCP address pool.

ip dhcp pool *pool-name*

no ip dhcp pool *pool-name*

Parameter description

Parameter	Description
pool-name	A string of characters and positive integers, for instance, mypool or 1.

Default	No DHCP address pool is defined by default.
Command mode	Global configuration mode.

Usage guidelines	Execute the command to enter into the DHCP address pool configuration mode: `DES-7200(dhcp-config)#` In this configuration mode, configure the IP address range, the DNS server and the default gateway.
Examples	The configuration example below defines a DHCP address pool with the name mypool0. `ip dhcp pool mypool0`

Related commands

Command	Description
host	Define the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp excluded-address	Define the IP addresses that the DHCP server cannot assign to the clients.
network (DHCP)	Define the network number and network mask of the DHCP address pool.

5.1.19 ip dhcp use class

Use this command to enable the CLASS to allocate addresses in the global configuration mode.The **no** form of this command can be used to disable the CLASS.

ip dhcp use class

no ip dhcp use class

Parameter description

Parameter	Description
-	-

Default	Enabled
Command mode	Global configuration mode.
Usage guidelines	N/A

Examples

The configuration example below enables the CLASS to allocate addresses.

```
DES-7200(config)# ip dhcp use class
```

Related commands

Command	Description
-	-

5.1.20 lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. The **no** form of this command can be used to restore it to the default configuration.

lease { *days* [*hours*] [*minutes*] | **infinite** }

no lease

Parameter description

Parameter	Description
days	Lease time in days
hours	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
minutes	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.
infinite	Infinite lease time.

Default

The lease is 1 days, by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.

Examples

The configuration example below sets the DHCP lease to 1 hour.

```
lease 0 1
```

The configuration example below sets the DHCP lease to 1 minute.

```
lease 0 0 1
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.21 netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the WINS server.

netbios-name-server *ip-address* [*ip-address2…ip-address8*]

netbios-name-server

Parameter description

Parameter	Description
ip-address	IP address of the WINS server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.

Default No WINS server is defined, by default.

Command mode DHCP address pool configuration mode.

Usage guidelines When more than one WINS server is defined, the former has higher priory. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

Examples The configuration example below specifies the WINS server 192.168.12.3 for the DHCP client.

```
netbios-name-server 192.168.12.3
```

Related

Command	Description

ip address dhcp	Enable the DHCP client on the interface to obtain the IP address.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.22 netbios-node-type

Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. The **no** form of this command can be used to delete the configuration of the NetBIOS node type.

netbios-node-type *type*

no netbios-node-type

Parameter description

Parameter	Description
type	Type of node in two modes: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: ■ 1: b-node. ■ 2: p-node. ■ 4: m-node. ■ 8: h-node. String: ■ b-node: broadcast node ■ p-node: peer-to-peer node ■ m-node: mixed node ■ h-node: hybrid node

Default No type of the NetBIOS node is defined, by default.

Command mode DHCP address pool configuration mode.

Usage guidelines

There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received.

By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.

Examples

The configuration example below sets the NetBIOS node of Microsoft DHCP client as Hybrid.

```
netbios-node-type h-node
```

Related commands

Command	Description
ip dhcp pool	Define the name of DHCP address pool and enter into the DHCP address pool configuration mode.
netbios-name-server	Configure the WINS name server of the Microsoft DHCP client NETBIOS.

5.1.23 network (DHCP)

Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the definition.

network *net-number net-mask*

no network

Parameter description

Parameter	Description
net-number	Network number of the DHCP address pool

net-mask	Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default.

Default No network number or network mask is defined, by default.

Command mode DHCP address pool configuration mode.

Usage guidelines

This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address.

The **show ip dhcp binding** command can be used to view the address assignment, and the **show ip dhcp conflict** command can be used to view the address conflict detection configuration.

Examples

The configuration example below defines the network number of the DHCP address pool as 192.168.12.0, and the network mask as 255.255.255.240.

```
network 192.168.12.0 255.255.255.240
```

Related commands

Command	Description
ip dhcp excluded-address	Define the IP addresses that the DHCP server cannot assign to the clients.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.24 next-server

Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. The **no** form of this command can be used to delete the definition of the startup server list.

next-server *ip-address* [*ip-address2…ip-address8*]

no next-server

Parameter description

Parameter	Description
ip-address	Define the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) Up to 8 startup servers can be configured.

Default

N/A.

Command mode

DHCP address pool configuration mode.

Usage guidelines

When more than one startup server is defined, the former will possess higher priory. The DHCP client will select the next startup server only when its communication with the former startup server fails.

Examples

The configuration example below specifies the startup server 192.168.12.4 for the DHCP client.

```
next-server 192.168.12.4
```

Related commands

Command	Description
bootfile	Define the default startup mapping file name of the DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.
ip help-address	Define the Helper address on the interface.
option	Configure the option of the DES-7200 DHCP server.

5.1.25 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the definition of option.

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

no option

Parameter description

Parameter	Description
code	Define the DHCP option codes.
ascii *string*	Define an ASCII string.
hex *string*	Define a hex string.
ip *ip-address*	Define an IP address list.

Default N/A.

Command mode Global configuration mode.

Usage guidelines

The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.

Examples

The configuration example below defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client.

```
DES-7200(dhcp-config)# option 19 hex 1
```

The configuration example below defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway

192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16.

```
option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0 192.168.12.16
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

5.1.26 relay agent information

Use this command to enter the Option82 matching information configuration mode in the global CLASS configuration mode. The **no** form of this command can be used to delete the Option82 matching information of the CLASS.

relay agent information

no relay agent information

Parameter description

Parameter	Description
-	-

Default N/A.

Command mode Global CLASS configuration mode.

Usage guidelines

After executing this command, it enters the Option82 matching information configuration mode which is shown as "`DES-7200 (config-dhcp-class-relayinfo)#`".

In this configuration mode, user can configure the class matching multiple Option82 information.

Examples

The configuration example below configures a global CLASS and enter the Option82 matching information configuration mode.

```
DES-7200(config)# ip dhcp class myclass
DES-7200(config-dhcp-class)# relay agent information
DES-7200(config-dhcp-class-relayinfo)#
```

Related

Command	Description

	ip dhcp class	Define a CLASS and enter the global CLASS configuration mode.

5.1.27 relay-information hex

Use this command to enter the Option82 matching information configuraiton mode. The **no** form of this command can be used to delete a piece of matching information.

relay-information hex *aabb.ccdd.eeff…* [*****]

no relay-information hex *aabb.ccdd.eeff…* [*****]

Parameter description

Parameter	Description
aabb.ccdd.eeff…[*]	Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching.

Default N/A.

Command mode Global CLASS configuration mode.

Usage guidelines N/A

Examples

The configuration example below configures a global CLASS which can match multiple Option82 infomration.

```
DES-7200(config)# ip dhcp class myclass
DES-7200(config-dhcp-class)# relay agent information
DES-7200(config-dhcp-class-relayinfo)#
relay-information
 hex 0102256535
DES-7200(config-dhcp-class-relayinfo)#
relay-information
 hex 010225654565
DES-7200(config-dhcp-class-relayinfo)#
relay-information
 hex 060225654565
DES-7200(config-dhcp-class-relayinfo)#
```

```
relay-information
 hex 060223*
```

Related commands

Command	Description
ip dhcp class	Define a CLASS and enter the global CLASS configuraiton mode.
relay agent information	Enter the Option82 matching information configuratin mode.

5.1.28 remark

Use this command to configure the identification which is used to describe the CLASS in this global CLASS configuraiton mode. The **no** form of this command can be used to delete the identification.

remark *class-remark*

no remark

Parameter description

Parameter	Description
class-remark	Information used to indentify the CLASS, it can be the character strings with space in them.

Default N/A.

Command mode Global CLASS configuration mode.

Usage guidelines N/A

Examples The configuration example below configures the identification information for a global CLASS.

```
DES-7200(config)# ip dhcp class myclass
DES-7200(config-dhcp-class)# remark used in #1 build
```

Related commands

Command	Description
ip dhcp class	Define a CLASS and enter the global CLASS configuration mode.

5.1.29 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in the global configuration mode. The **no** form of this command can be used to disable the DHCP server and the DHCP relay.

service dhcp

no service dhcp

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.
Examples	In the following configuration example, the device has enabled the DHCP server and the DHCP relay feature. `service dhcp`

Related commands

Command	Description
show ip dhcp server statistics	Show various statistics information of the DHCP server.

5.2 Showing and Monitoring Commands

5.2.1 clear ip dhcp binding

Use this command to clear the DHCP binding table in the privileged user mode:

clear ip dhcp binding { * | *ip-address* }

Parameter description

Parameter	Description
*	Delete all DHCP bindings.

	ip-address	Delete the binding of the specified IP addresses.

Default N/A.

Command mode Privileged mode.

Usage guidelines This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the **no ip dhcp pool** command.

Examples The example below clears the DHCP binding with the IP address 192.168.12.100.

```
clear ip dhcp binding 192.168.12.100
```

Related commands

Command	Description
show ip dhcp binding	Show the address binding of the DHCP server.

5.2.2 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record in the privileged user mode:

clear ip dhcp conflict { * | *ip-address* }

Parameter description

Parameter	Description
*	Delete all DHCP address conflict records.
ip-address	Delete the conflict record of the specified IP addresses.

Default N/A.

Command mode Privileged mode.

Usage guidelines	The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The **clear ip dhcp conflict** can be used to delete the history conflict record.
Examples	The example below clears all address conflict records. `clear ip dhcp conflict *`

Related commands

Command	Description
ip dhcp ping packets	Define the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
show ip dhcp conflict	Show the address conflict that the DHCP server detects when it assigns an IP address.

5.2.3 clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in the privileged user mode.

clear ip dhcp server statistics

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The **clear ip dhcp server statistics** command can be used to delete the history counter record and carry out the statistics starting from scratch.
Examples	The example below clears the statistics record of the DHCP server. `clear ip dhcp server statistics`

Related commands

Command	Description
show ip dhcp server statistics	Show the statistics record of the DHCP server.

5.2.4 debug ip dhcp client

Use this command to carry out the DHCP client debugging in the privileged user mode:

debug ip dhcp client

no debug ip dhcp client

Parameter description N/A.

Default Disabled.

Command mode Privileged mode.

Usage guidelines This command is used to show the main message content of the DHCP client during the interaction of the servers and the processing status.

Examples The example below turns on the debugging switch of the DHCP client in the equipment.

```
debug ip dhcp client
```

5.2.5 debug ip dhcp server

Use this command to carry out the DHCP Server debugging in the privileged user mode:

debug ip dhcp server { **event** | **packet** }

no debug ip dhcp server { **event** | **packet** }

Parameter description

Parameter	Description
event	Show the DHCP message.
packet	Show the DHCP packet.

Default Disabled.

Command mode	Privileged mode.
Usage guidelines	This command is used to show the main message content of the dhcp server during the interaction of the clients and the processing status.
Examples	The example below turns on the debugging switch of the DHCP server in the equipment. `DES-7200# debug ip dhcp server packet`

5.2.6 show dhcp lease

Use this command to show the lease information of the IP address obtained by the DHCP client.

show dhcp lease

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address.

Examples	The following is the result of the **show dhcp lease**.
	`DES-7200# show dhcp lease`
	`Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0`
	`Temp sub net mask: 255.255.255.0`
	`DHCP Lease server: 192.168.5.70, state: 3 Bound`
	`DHCP transaction id: 168F`
	`Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs`
	`Temp default-gateway addr: 192.168.5.1`
	`Next timer fires after: 00:04:29`
	`Retry count: 0 Client-ID:`

redgaint-00d0.f8fb.5740-Fa0/0

5.2.7 show ip dhcp binding

Use this command to show the binding condition of the DHCP address.

show ip dhcp binding [*ip-address*]

Parameter description

Parameter	Description
ip-address	(Optional) Only show the binding condition of the specified IP addresses.

Default

N/A.

Command mode

Privileged mode.

Usage guidelines

If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address.

Examples

The following is the result of the **show ip dhcp binding**.

```
DES-7200# show ip dhcp binding
IP address    Client-Identifier/  Lease expiration  Type
              Hardware address
192.168.1.2         00d0.f866.4777                  IDLE
Manual
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	The IP address to be assigned to the DHCP client.
Client-Identifier /Hardware address	The client identifier or hardware address of the DHCP client.

Lease expiration	The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively.
Type	The type of the address binding.The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual.

Related commands

Command	Description
clear ip dhcp binding	Clear the DHCP address binding table.

5.2.8 show ip dhcp conflict

Use this command to show the conflict history record of the DHCP sever.

show ip dhcp conflict

Parameter description N/A.

Default N/A.

Command mode Privileged mode.

Usage guidelines This command can show the conflict address list and excluded address list detected by the DHCP server.

Examples The following is the output result of the **show ip dhcp conflict** command.

```
DES-7200# show ip dhcp conflict
IP address    Detection Method
```

```
192.168.12.1    Ping

dhcpd excluded ipaddress
 192.168.12.100
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	**The IP addresses which cannot be assigned to the DHCP client.**
Detection Method	**The conflict detection method.**
dhcpd excluded ipaddress	**The range of excluded addresses.**

Related commands

Command	Description
clear ip dhcp confict	Clear the DHCP conflict record.

5.2.9 show ip dhcp server statistics

Use this command to show the statistics of the DHCP server.

show ip dhcp server statistics

Parameter description N/A.

Default N/A.

Command mode Privileged mode.

Usage guidelines This command shows the statistics of the DHCP server.

Examples

The following is the output result of the **show ip dhcp server statistics** command.

```
DES-7200# show ip dhcp server statistics
Lease count             7
Address pools           4
Automatic bindings      4
Manual bindings         0
```

```
Expired bindings         0
Malformed messages 2
Message                 Received
BOOTREQUEST              216
DHCPDISCOVER             33
DHCPREQUEST              25
DHCPDECLINE              0
DHCPRELEASE              1
DHCPINFORM               150
Message                 Sent
BOOTREPLY                16
DHCPOFFER                9
DHCPACK                  7
DHCPNAK                  0
```

The meaning of various fields in the show result is described as follows.

Field	Description
Address pools	Number of address pools.
Lease count	Number of allocated lease.
Automatic bindings	Number of automatic address bindings.
Manual bindings	Number of manual address bindings.
Expired bindings	Number of expired address bindings.
Malformed messages	Number of malformed messages received by the DHCP.
Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.

Related commands

Command	Description
clear ip dhcp server statistics	Delete the DHCP server statistics.

6 DHCP Relay Configuration Commands

6.1 DHCP Relay Configuration Commands

6.1.1 ip dhcp relay check server-id

Use this command to enable the **ip dhcp relay check** *server-id* function. The **no** form of this command is used to disable the **ip dhcp relay check** *server-id* function.

[**no**] **ip dhcp relay check server-id**

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Switch will select the server to be sent according to server-id option when forwarding DHCP REQUEST via this command. Wihout this comand configured, the switch forwards the DHCP REQUEST to all configured DHCP servers.

Examples	The following example enables the ip dhcp relay check server-id function.
	`DES-7200# configure terminal`
	`DES-7200(config)# ip dhcp relay check server-id`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.

Platform description	This command is only supported by the switches.

6.1.2 ip dhcp relay information option dot1x

Use this command to enable the **dhcp option dot1x** function.. The **no** form of the command is used to disable the **dhcp option dot1x** function.

[**no**] **ip dhcp relay information option dot1x**

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	It is necessary to enable the DHCP Relay, and combine with the 802.1x related configuration to configure this command.

Examples	The following example enables the DHCP option dot1x function on the device.
	`DES-7200# configure terminal`
	`DES-7200(config)# ip dhcp relay information option dot1x`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.
ip dhcp relay information option dot1x access-group	Configure the option dot1x acl.

Platform description	This command is only supported by switches.

6.1.3 ip dhcp relay information option dot1x access-group

Use this command to configure the **dhcp option dot1x acl**. The **no** form of this command is used to disable the **dhcp option dot1x acl**.

[**no**] **ip dhcp relay information option dot1x access-group** *acl-name*

Default	No ACL is associated with.

Command mode

Global configuration mode.

Usage guidelines

Be sure that the ACL does not conflict with the existing ACE of the configured ACL on the interface.

Examples

The following example enables the dhcp option dot1x acl function.

```
DES-7200# configure terminal
DES-7200(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
DES-7200(config-ext-nacl)# permit ip any host 192.168.3.1
```

//Permit sending the packets to the gateway.

```
DES-7200(config-ext-nacl)# permit ip any host 192.168.4.1
DES-7200(config-ext-nacl)# permit ip any host 192.168.5.1
DES-7200(config-ext-nacl)# permit ip host 192.168.3.1 any
```

// Permit the communication between the packets whose source IP address is that of the gateway.

```
DES-7200(config-ext-nacl)# permit ip host 192.168.4.1 any
DES-7200(config-ext-nacl)# permit ip host 192.168.5.1 any
DES-7200(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
```

//Deny the exchange between the unauthenticated users.

```
DES-7200(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.5.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255
DES-7200(config-ext-nacl)# exit
DES-7200(config)# ip dhcp relay information option dot1x access-group DenyAccessEachOtherOfUnauthrize
```

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.
ip dhcp relay information option dot1x	Enable the DHCP option dot1x function.

Platform description

This command is only supported by switches.

6.1.4 ip dhcp relay information option82

Use this command to configure to enable the **ip dhcp relay information option82** function. The **no** form of this command is used to disable the **ip dhcp relay information option82** function.

[**no**] **ip dhcp relay information option82**

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

This command is exclusive with the **option dot1x** command.

Examples

The following example enables the option82 function on the DHCP relay.

```
DES-7200# configure terminal
DES-7200(config)# Ip dhcp relay information option82
```

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.
ip dhcp relay information option dot1x	Enable the DHCP option dot1x function.

Platform description

This command is only supported by switches.

6.1.5 ip dhcp relay information option vpn

Use this command to configure to enable the DHCP Relay Aware VRF function on the DHCP Relay device. The **no** form of this command is used to disable this function.

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	This command is exclusive with the **option dot1x** and **option82** command.

Examples	The following example enables the DHCP Relay Aware VRF function on the DHCP Relay device.
	`DES-7200# configure terminal`
	`DES-7200(config)#Ip dhcp relay information option vpn`

Related commands

Command	Description
ip dhcp relay information option82	Enable the DHCP option82 function.
ip dhcp relay information option dot1x	Enable the DHCP option dot1x function.

Platform description	This command is only supported by switches.

6.1.6 ip dhcp relay suppression

Use this command to enable the DHCP binding globally. The **no** form of this command disables the DHCP binding globally and enables the **DHCP relay** suppression on the port.

[**no**] **ip dhcp relay suppression**

Default configuration	Disabled.

Command mode	Interface configuration mode.
Usage guidelines	After executing this command, the system will not relay the DHCP request message on the interface.

Examples	The following example enables the relay suppression function on the interface 1.
	`DES-7200# configure terminal`
	`DES-7200(config)# interface fastEthernet 0/1`
	`DES-7200(config-if)# ip dhcp relay suppression`
	`DES-7200(config-if)# exit`
	`DES-7200(config)#`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.

Platform description	This command is only supported by switches.

6.1.7 ip helper-address

Use this command to add an IP address of the DHCP server. The **no** form of this command deletes an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

[**no**] **ip helper-address** [**vrf** *vrf-name*]*A.B.C.*

Default	N/A.
Command mode	Global configuration mode, interface configuration mode.

Usage guidelines	Up to 20 DHCP server can be configured globally or on a layer-3 interface. One DHCP request of this interface will be sent to these servers. You can select one for confirmation. The global configuration and port-based configuration of the vrf are slightly different. In the global configuration mode, if the vrf is not specified, the default address of the current server does not belong to any vrf. In the port-based configuration, if the vrf is not specified, the current default server and port configurations belong to the same vrf.

Examples	The following example configures the addresses for two servers.
	1. Set the IP address for the global server to 192.168.1.1
	2. Set the IP address for the vrf instance-based server delp1 to 192.168.2.1
	`DES-7200# configure terminal`
	`DES-7200(config)# ip helper-address 192.168.1.1`
	`DES-7200(config)# ip helper-address vrf dep1 192.168.2.1`

Related commands

Command	Description
service dhcp	Enable the DHCP relay.

6.1.8 service dhcp

Use this command to enable the DHCP relay in the global configuration mode. The **no** form of this command can disable the DHCP relay.

service dhcp

no service dhcp

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP response packets to the DHCP client, serving as the relay for DHCP packets.
Examples	In the following configuration example, the device has

enabled the DHCP server and the DHCP relay.

```
DES-7200# configure terminal
DES-7200(config)# service dhcp
```

Related commands

Command	Description
ip helper-address	Add an IP address of the DHCP server.

7 UDP-Helper Module Configuration Commands

7.1 Configuration Related Commands

7.1.1 ip forward-protocol

Use this command to configure the UDP port to enable forwarding. Use the **no** form of this command to disable forwarding on the UDP port.

ip forward-protocol udp [*port* | **tftp | domain | time | netbios-ns | netbios-dgm | tacacs]**

no ip forward-protocol udp [*port* | **tftp | domain | time | netbios-ns | netbios-dgm | tacacs]**

Parameter description

Parameter	Description
port	Port to enable forwarding. If this parameter is not specified, the broadcast message from the ports 69,53,37,137,138,49 will be forwarded by default.
tftp	Trivial File Transfer Protocol(69) Forward the broadcast message from port 69.
domain	Domain Name System(53) Forward the broadcast message from port 53.
time	Time service(37) Forward the broadcast message from port 37.
netbios-ns	NetBIOS Name Service(137) Forward the broadcast message from port 137.
netbios-dgm	NetBIOS Datagram Service(138) Forward the broadcast message from port 138.
tacacs	TAC Access Control System(49)

		Forward the broadcast message from port 49.

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	Enabling the UDP-Helper function will forward the broadcast message of the UDP ports 69,53,37,137,138,49 without any additional configuration, by default.
Examples	`DES-7200(config)# ip forward-protocol udp 134`

Related commands

Command	Description
udp-helper enable	Enable the forwarding of the UDP broadcast message.
ip forward-protocol	Configure the UDP port to enalbe forwarding.

7.1.2 ip helper-address

Use this command to configure the destination server which the UDP broadcast message will be forwarded to. Use the **no** form of this command to delete the destination server.

ip helper-address *address*

no ip helper-address *[address]*

Parameter description

Parameter	Description
address	IP address of the destination server in the dotted decimal format. Each interface can support up to 20 server addresses.

Default configuration	N/A.

Command mode	Interface configuration mode.
Usage guidelines	Up to 20 destination servers can be configured on an interface. Once the forwarding destination server is configured someone an interface and UDP-Helper is enabled, the broadcast message of the specified port received from this interface will be sent to the destination server configured on this interface in unicast form. Use the **no ip helper-address** to remove the forwarding destination server.
Examples	The following is an example of configuring the destination server where the UDP broadcast message will be forwarded to. `DES-7200(config-if)# ip helper-address 192.168.100.1`

Related commands

Command	Description
ip forward-protocol	Configure the specified UDP port to enable forwarding.

7.1.3 udp-helper enable

Use this command to enable the forwarding function of the UDP broadcast message. The **no udp-helper enable** command is used to disable the forward function of the UDP broadcast message.

By default, the forwarding of the UDP broadcast message is disabled.

udp-helper enable

no udp-helper enable

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.

Usage guidelines

Enable the forwarding function of UDP-Helper. The UDP broadcast messages from the port 69,53,37,137,138,49 are forwarded by default.

Examples

The following is an example of enabling the UDP forwarding function.

```
DES-7200(config)# udp-helper enable
```

Related commands

Command	Description
Ip forward-protocol	Configure the UDP port to enable the forwarding funciton.

8 DHCPv6 Server Configuration Commands

8.1 Configuration Related Commands

8.1.1 clear ipv6 dhcp binding

Use this command to clear the DHCPv6 binding information.

clear ipv6 dhcp binding [*ipv6-address*]

Parameter description

Parameter	Description
ipv6-address	Set the IPv6 address or the prefix.

Default Settings

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

If the *ipv6-address* is not specified, all DHCPv6 binding information are cleared. If the *ipv6-address* is specified, the binding information for the specified address is cleared.

Examples

The following example shows how to clear the DHCPv6 binding information:

```
DES-7200(config)# clear ipv6 dhcp binding
```

Platform description

N/A

8.1.2 clear ipv6 dhcp server statistics

Use this command to clear the DHCPv6 server statistics.

clear ipv6 dhcp server statistics

Parameter description

Parameter	Description
-	-

Default Settings

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to clear the DHCPv6 server statistics.

Examples

The following example shows how to clear the DHCPv6 server statistics:

```
DES-7200(config)# clear ipv6 dhcp server statistics
```

Platform description

N/A

8.1.3 dns-server

Use this command to set the DNS Server list information for the DHCPv6 Server. Use the **no** form of this command to remove the configuration.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Parameter description

Parameter	Description
ipv6-address	Set the IPv6 address or the DNS server.

Default Settings

By default, no DNS server list is configured.

Command mode	DHCPv6 pool configuration mode.
Usage guidelines	To configure several DNS Server addresses, use the **dns-server** command for several times. The newly-configured DNS Server address will not overwrite the former ones.
Examples	`DES-7200(config-dhcp)# dns-server 2008:1::1`

Related commands

Command	Description
domain-name	Set the DHCPv6 domain name information.
ipv6 dhcp pool	Set a DHCPv6 pool.

Platform description	N/A

8.1.4 domain-name

Use this command to set the domain name for the DHCPv6 server. Use the **no** form of this command to remove the domain name.

domain-name *domain*

no domain-name *domain*

Parameter description

Parameter	Description
domain	Set the domain name.

Default Settings	By default, no domain name is configured.
Command mode	DHCPv6 pool configuration mode.
Usage	To configure several domain names, use the

guidelines	**domain-name** command for several times. The newly-configured domain name will not overwrite the former ones.

Examples

```
DES-7200(config-dhcp)# domain-name example.com
```

Related commands

Command	Description
dns-server	Set the DHCPv6 DNS server list.
ipv6 dhcp pool	Set the DHCPv6 pool.

Platform description	N/A

8.1.5 iana-address prefix

Use this command to set the IA_NA address prefix for the DHCPv6 Server. Use the **no** form of this command to remove the IA_NA address prefix.

iana-address prefix *ipv6-prefix/prefix-length* [**lifetime** {*valid-lifetime* | *preferred-lifetime*}]

no iana-address prefix

Parameter description

Parameter	Description
ipv6-prefix/prefix-length	Set the IPv6 prefix and prefix length.
lifetime	Set the lifetime of the address allocated to the client. With the keyword **lifetime** configured, both parameters *valid-lifetime* amd *preferred-lifetime* shall be configured.
valid-lifetime	Set the valid lifetime of using the allocated address for the client.
preferred-lifetime	Set the preferred lifetime of the address allocated to the client.

Default Settings	By default, no IA_NA address prefix is configured; The default *valid-lifetime* is 3600s(1 hour). The default *preferred-lifetime is* 3600s(1 hour).
Command mode	DHCPv6 pool configuration mode.
Usage guidelines	This command is used to set the IA_NA address prefix for the DHCPv6 Server, and allocate the IA_NA address to the client. The Server attempts to allocate a usable address within the IA_NA address prefix range to the client upon receiving the IA_NA address request from the client. That address will be allocated to other clients if the client no longer uses that address again.
Examples	`DES-7200(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000DES-7200(config-if)# ip verify urpf drop-rate notify`

Related commands

Command	Description
ipv6 dhcp pool	Set the DHCPv6 pool.
show ipv6 dhcp pool	Show the DHCPv6 pool information.

Platform description	N/A

8.1.6 ipv6 dhcp server

Use this command to enable the DHCPv6 server on the interface. Use the **no** form of this command to disable this function.

ipv6 dhcp server *poolname* [**rapid-commit**] [**preference** *value*]

no ipv6 dhcp server

Parameter description

Parameter	Description
poolname	Define the DHCPv6 pool name.

rapid-commit	Allow to use the two-message interaction process.
preference *value*	Set the preference level for the advertise message. The valid range is 1-100 and the default value is 0.

Default Settings

Disabled

Command mode

Interface configuration mode.

Usage guidelines

Use the **ipv6 dhcp server** command to enable the DHCPv6 service.

Configuring the keyword **rapid-commit** allows the two-message interaction for the server and the client when allocating the address prefix and setting other configurations. With this keyword configured, if the client solicit message includes the **rapid-commit** item, the DHCPv6 Server will send the Reply message immediately.

DHCPv6 Server carries with the **preference** value when sending the advertise message if the **preference** level is not 0.

If the **preference** level is 0, the advertise message will not include this field. If the **preference** value is 255, the client sends the request message to the server to obtain the configurations.

DHCPv6 Client, Server and Relay functions are exclusive, and only one of the functions can be configured on the interface.

Examples

```
DES-7200(config)# interface fastethernet 0/1
DES-7200(config-if)# ipv6 dhcp server pool1
```

Related commands

Command	Description
ipv6 dhcp pool	Set the DHCPv6 pool.
show ipv6 dhcp pool	Show the DHCPv6 pool information.

Platform description	N/A

8.1.7 ipv6 dhcp pool

Use this command to set the DHCPv6 server pool. Use the **no** form of this command to remove the information pool.

ipv6 dhcp pool *poolname*

no ipv6 dhcp pool *poolname*

Parameter description

Parameter	Description
poolname	Define the DHCPv6 pool name.

Default Settings	By default, the DHCPv6 server information pool is not configured.
Command mode	Global configuration mode.

Usage guidelines

This command is used to create a DHCPv6 Server configuration pool. After configuring this command, it enters the DHCPv6 pool configuration mode, in which the administrator can set the pool parameters, such as the prefix and the DNS Server information, ect.

After creating the DHCPv6 Server configuration pool, use the **ipv6 dhcp server** command to associate the pool and the DHCPv6 Server on one interface.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ipv6 dhcp pool pool1
DES-7200(config-dhcp)#
```

Related commands

Command	Description
ipv6 dhcp server	Enable the DHCPv6 server function on the interface.
show ipv6 dhcp pool	Show the DHCPv6 pool information.

Platform description	N/A

8.1.8 prefix-delegation

Use this command to set the static binding address prefix information for the DHCPv6 server. Use the **no** form of this command to delete the address prefix information.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [*lifetime*]

no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [*lifetime*]

Parameter description

Parameter	Description
ipv6-prefix/prefix-length	Set the IPv6 address prefix and the prefix length.
client-DUID	Set the client DUID.
lifetime	Set the interval of using the prefix by the client.

Default Settings

By default, no address prefix information is configured.

Command mode

DHCPv6 pool configuration mode.

Usage guidelines

The administrator uses this command to manually set the address prefix information list for the client IA_PD and set the valid lifetime for those prefixes.

The parameter *client-DUID* allocates the address prefix to the first IA_PD in the specified client.

Before receiving the request message for the address prefix from the client, DHCPv6 Server searches for the corresponding static binding first. If it succeeds, the server returns to the static binding; otherwise, the server will attempt to allocate the address prefix from other prefix information sources.

Examples

```
DES-7200(config-dhcp)# prefix-delegation 2008:2::/64
0003000100d0f82233ac
```

Related commands

Command	Description
ipv6 dhcp pool	Set a DHCPv6 pool.
ipv6 local pool	Set a local prefix pool.
prefix-delegation pool	Specify the DHCPv6 local prefix pool.
show ipv6 dhcp pool	Show the DHCPv6 pool information.

Platform description

N/A

8.1.9 prefix-delegation pool

Use this command to specify the local prefix pool for the DHCPv6 server. Use the **no** form of this command to remove the local prefix pool.

prefix-delegation pool *poolname* [**lifetime** {*valid-lifetime* | *preferred-lifetime*}]

no prefix-delegation pool *poolname*

Parameter description

Parameter	Description
poolname	Set the local prefix pool name.
lifetime	Set the lifetime of the address prefix allocated to the client. With the keyword **lifetime** configured, both parameters *valid-lifetime* amd *preferred-lifetime* shall be configured.
valid-lifetime	Set the valid lifetime of using the allocated address prefix for the client.
preferred-lifetime	Set the preferred lifetime of the address prefix allocated to the client.

Default Settings

By default, no address prefix pool is specified.

The default *valid-lifetime* is 3600s(1 hour).

The default *preferred-lifetime is* 3600s(1 hour).

Command mode	DHCPv6 pool configuration mode.
Usage guidelines	Use the **prefix-delegation pool** command to set the prefix pool for the DHCPv6 Server and allocate the prefix to the client. Use the **ipv6 local pool** command to set the prefix pool. The Server attempts to allocate a usable prefix from the prefix pool to the client upon receiving the prefix request from the client. That prefix will be allocated to other clients if the client no longer uses that prefix again.
Examples	`DES-7200(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000`

Related commands

Command	Description
ipv6 dhcp pool	Set a DHCPv6 pool.
ipv6 local pool	Set a local prefix pool.
prefix-delegation	Staticlly bind the client with the address prefix.
show ipv6 dhcp pool	Show the DHCPv6 pool information.

Platform description	N/A

8.2 Showing Related Commands

8.2.1 show ipv6 dhcp

Use this command to show the device DUID.

show ipv6 dhcp

Parameter description

Parameter	Description
-	-

Default Settings	N/A
Command mode	Privileged EXEC mode.
Usage guidelines	The server, client and relay on the same device share a DUID.
Examples	`DES-7200# show ipv6 dhcp` `This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0`
Platform description	N/A

8.2.2 show ipv6 dhcp binding

Use this command to show the address binding information for the DHCPv6 server.

show ipv6 dhcp binding [*ipv6-address*]

Parameter description

Parameter	Description
ipv6-address	Set the IPv6 address or the prefix.

Default Settings	N/A
Command mode	Privileged EXEC mode.
Usage guidelines	If the *ipv6-address* is not specified, all prefixes dynamically assigned to the client and IANA address binidng information are shown. If the *ipv6-address* is specified, the binding information for the specified address is shown.
Examples	`DES-7200# show ipv6 dhcp binding` `Client DUID: 00:03:00:01:00:d0:f8:22:33:ac`

```
IAPD: iaid 0, T1 1800, T2 2880
  Prefix: 2001:20::/72
         preferred lifetime 3600, valid lifetime 3600
      expires at Jan 1 2008 2:23 (3600 seconds)
```

Platform description N/A

8.2.3 show ipv6 dhcp interface

Use this command to show the DHCPv6 interface information.

show ipv6 dhcp interface *[interface-name]*

Parameter description

Parameter	Description
interface-name	Set the interface name.

Default Settings N/A

Command mode Privileged EXEC mode.

Usage guidelines If the *interface-name* is not specified, all DHCPv6 interface information are shown. If the *interface-name* is specified, the specified interface information is shown.

Examples

```
DES-7200# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool dhcp-pool
  Rapid-Commit: disable
```

Platform description N/A

8.2.4 show ipv6 dhcp pool

Use this command to show the DHCPv6 pool information

show ipv6 dhcp pool *[poolname]*

Parameter description

Parameter	Description
poolname	Define the DHCPv6 pool name.

Default Settings	N/A
Command mode	Privileged EXEC mode.
Usage guidelines	If the *poolname* is not specified, all DHCPv6 interface information are shown. If the *poolname* is specified, the specified interface information is shown.
Examples	DES-7200# **show ipv6 dhcp pool** DHCPv6 pool: dhcp-pool DNS server: 2011:1::1 DNS server: 2011:1::2 Domain name: example.com
Platform description	N/A

8.2.5 show ipv6 dhcp server statistics

Use this command to show the DHCPv6 server statistics.

show ipv6 dhcp server statistics

Parameter description	Parameter	Description
	-	-

Default Settings	N/A
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the DHCPv6 server statistics.
Examples	DES-7200# **show ipv6 dhcp server statistics** DHCPv6 server statistics:

```
Packet statistics:

DHCPv6 packets received:          7

Solicit received:                 7

Request received:                 0

Confirm received:                 0

Renew received:                   0

Rebind received:                  0

Release received:                 0

Decline received:                 0

Relay-forward received:           0

Information-request received:     0

Unknown message type received:    0

Error message received:           0


DHCPv6 packet sent:               0

Advertise sent:                   0

Reply sent:                       0

Relay-reply sent:                 0

Send reply error:                 0

Send packet error:                0


Binding statistics:

Bindings generated:               0

IAPD assigned:                    0

IANA assigned:                    0


Configuration statistics:

DHCPv6 server interface:          1
```

```
DHCPv6 pool:                    0

DHCPv6 iapd binding:             0
```

Related commands

Command	Description
ipv6 dhcp pool	Set a DHCPv6 pool.

Platform description

N/A

9 DHCPv6 Client Configuration Commands

9.1 Configuration Related Command

9.1.1 ipv6 dhcp client pd

Use this command to enable the DHCPv6 client and request for the prefix address information. Use the **no** form of this command to disable the prefix address request.

ipv6 dhcp client pd ***prefix-name*** [rapid-commit]

no ipv6 dhcp client pd

Parameter description

Parameter	Description
prefix-name	Define the IPv6 prefix name.
rapid-commit	Allow the simplified interaction process.

Default Disabled

Command mode Interface configuration mode.

Usage guidelines

With the DHCPv6 client mode disabled, use this command to enable the DHCPv6 client mode on the interface.

With the **ipv6 dhcp client pd** command enabled, the DHCPv6 client sends the prefix request to the DHCPv6 server

The keyword **rapid-commit** allows the client and the server two-message interaction process. With this keyword configured, the solicit message sent by the client includes the **rapid-commit** item.

Examples The following example shows how to enable the prefix information request on the interface:

	DES-7200(config)# **interface fastethernet** *0/1* DES-7200(config-if)# **ipv6 dhcp client pd** *pd_name*

Related commands

Command	Description
clear ipv6 dhcp client	Reset the DHCPv6 client function on the interface.
show ipv6 dhcp interface	Show the DHCPv6 interface configuration.

9.2 Showing Related Commands

9.2.1 show ipv6 dhcp

Use this command to show the device DUID information.

show ipv6 dhcp

Parameter description

Parameter	Description
-	-

Default N/A.

Command mode Privileged EXEC mode / Global / Interface configuration mode.

Usage guidelines One DUID is shared by the server, client and relay on the same device.

Examples

```
DES-7200# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID):
00:03:00:01:00:d0:f8:22:33:b0
```

9.2.2 show ipv6 dhcp interface

Use this command to show the DHCPv6 interface information.

show ipv6 dhcp interface [***interface-type interface-number***]

Parameter description

Parameter	Description
interface-type interface-number	Set the interface type and the interface number.

Default	N/A.
Command mode	Privileged EXEC mode / Global / Interface configuration mode.
Usage guidelines	If the *interface-type interface-number* is not defined, show the information of all DHCPv6 interfaces. If the *interface-type interface-number* is defined, show the information of this interface.

Examples	`DES-7200# show ipv6 dhcp interface`
	`VLAN 1 is in server mode`
	`  Server pool dhcp-pool`
	`  Rapid-Commit: disable`

9.2.3 clear ipv6 dhcp client

Use this command to reset the DHCPv6 client.

clear ipv6 dhcp client ***interface-type interface-number***

Parameter description

Parameter	Description
interface-type interface-number	Set the interface type and the interface number.

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to reset the DHCPv6 client, which may lead the client to request for the configurations from the server again.
Examples	`DES-7200# clear ipv6 dhcp client vlan 1`

10 DHCPv6 Relay Agent Configuration Commands

10.1 Configuration Related Command

10.1.1 ipv6 dhcp relay destination

Use this command to enable the DHCPv6 Relay Agent function and specify the destination address and the destination interface. Use the **no** form of this command to disable this function or remove the destination address.

ipv6 dhcp relay destination *ipv6-address [interface-type interface-number]*

no ipv6 dhcp relay destination *ipv6-address [interface-type interface-number]*

Parameter description

Parameter	Description
ipv6-address	Specify the Relay Agent destination address.
interface-type	(Optional) Specify the destination interface type.
interface-number	(Optional) Specify the destination interface number.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines	With the DHCPv6 Relay function enabled on the interface, all DHCPv6 client messages will be encapsulated and forwarded to the specified interface and the configured destination addresses. **Caution** ✧ The **dhcpv6 relay destination** command can only be enabled on the layer-3 interface. ✧ There can be up to 20 Relay Agent Destinations on one device. ✧ The interface number must be defined if the destination address is the multicast address.

Examples	The following example shows how to enable DHCPv6 Relay service on the interface VLAN1 and specify the destination address 3001::2:
	`DES-7200#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`DES-7200(config)#interface vlan 1`
	`DES-7200(config-if)#ipv6 dhcp relay destination 3001::2`
	`DES-7200(config-if)#end`

Related commands	**Command**: **show ipv6 dhcp relay destination** { **all** | **interface** *interface-type interface-number* } **Description**: Show the current Relay destination address list.
Platform description	N/A

10.2 Showing Related Commands

10.2.1 show ipv6 dhcp relay destination

Use this command to show the DHCPv6 Relay Agent destination address and interface information.

show ipv6 dhcp relay destination

Parameter description

Parameter	Description
all	Show all destination address and interface information.
interface *interface-type interface-number*	Show the specified destination address and interface information.

Default N/A.

Command mode Privileged EXEC mode

Usage guidelines N/A

Examples The following example shows all current Relay destination address configurations:

```
DES-7200# show ipv6 dhcp relay destination all
Interface: Vlan1
Destination address(es)      Output Interface
3001::2
FF02::1:2                              Vlan2
```

Platform description N/A

10.2.2 show ipv6 dhcp relay statistics

Use this command to show the packet sending and receiving condition with the DHCPv6 Relay function enabled.

show ipv6 dhcp relay statistics

Parameter description

Parameter	Description
-	-

Default N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	N/A

Examples

```
DES-7200# show ipv6 dhcp relay statistics
Packets dropped             :  2
   Error                   :  2
   Excess of rate limit     :  0
Packets received            :  28
   SOLICIT                 :  0
   REQUEST                 :  0
   CONFIRM                 :  0
   RENEW                   :  0
   REBIND                  :  0
   RELEASE                 :  0
   DECLINE                 :  0
   INFORMATION-REQUEST      :  14
   RELAY-FORWARD           :  0
   RELAY-REPLY             :  14
Packets sent                :  16
   ADVERTISE               :  0
   RECONFIGURE             :  0
   REPLY                   :  8
   RELAY-FORWARD           :  8
   RELAY-REPLY             :  0
```

Related commands

Command	Description
clear ipv6 dhcp relay statistics	Clear the statistical information.

Platform description	N/A

10.2.3 clear ipv6 dhcp relay statistics

Use this command to clear the packet sending and receiving condition with the DHCPv6 Relay function enabled.

clear ipv6 dhcp relay statistics

Parameter description

Parameter	Description
-	-

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A

Examples

```
DES-7200# clear ipv6 dhcp relay statistics
```

Related commands

Command	Description
show ipv6 dhcp relay statistics	Show the statistical information.

Platform description N/A

11 DNS Module Configuration Commands

11.1 Configuring Related Commands

11.1.1 ip domain-lookup

Use this command to enable the DNS to carry out the domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

ip domain-lookup

no ip domain-lookup

Default configuration	Enabled.
Command mode	Global configuration mode.
Usage guidelines	This command enables the domain name resolution function.
Examples	The following example enables the DNS domain name resolution function. `DES-7200(config)# ip domain-lookup`

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

11.1.2 ip host

Use this command to configure the mapping of the host name and the IP address by manual. Use the **no** form of the command to remove the host list.

ip host *host-name ip-address*

no ip host *host*-name *ip-address*

Parameter description

Parameter	Description
host-name	The host name of the equipment
ip-address	The IP address of the equipment

Command mode

Global configuration mode.

Usage guidelines

To delete the host list, use the **no ip host** *host-name ip-address* command.

Examples

```
DES-7200(config)# ip host switch 192.168.5.243
```

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

11.1.3 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server {*ip-address* | *ipv6-address}*

no ip name-server [*ip-address*| *ipv6-address*]

Parameter description

Parameter	Description
ip-address	The IP address of the domain name server.
ipv6-address	The IPv6 address of the domain name server.

Default configuration

N/A.

Command mode	Global configuration mode.
Usage guidelines	Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response. Up to 6 DNS servers are supported. You can delete a DNS server with the *ip-address* option or all the DNS servers.

Examples	`DES-7200(config)# ip name-server 192.168.5.134`
	`DES-7200(config)# ip name-server`
	`2001:0DB8::250:8bff:fee8:f800 2001:0DB8:0:f004::1`

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

11.1.4 ipv6 host

Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the **no** form of the command to remove the host list.

ipv6 host *host-name ipv6-address*

no ipv6 host *host*-name *ipv6-address*

Parameter description

Parameter	Description
host-name	The host name of the equipment
ipv6-address	The IPv6 address of the equipment

Command mode	Global configuration mode.
Usage guidelines	To delete the host list, use the **no ipv6 host** *host-name ipv6-address* command.
Examples	`DES-7200(config)# ipv6 host switch` `2001:0DB8:700:20:1::12`

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

11.2 Show Related Commands

11.2.1 clear host

Use this command to clear the dynamically learned host name in the privileged user mode.

clear host [*host-name*]

Parameter description

Parameter	Description
host-name	Delete the dynamically learned host. "*" denotes to clear all the dynamically learned host names.

Command mode

Privileged mode.

Usage guidelines

You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.

Examples

The following configuration will delete the dynamically learned mapping records from the host name-IP address buffer table.

```
clear host *
```

Related commands

Command	Description
show hosts	Show the host name buffer table.

11.2.2 show hosts

Use this command to display DNS configuration.

show hosts [*hostname*]

Command mode

Privileged mode.

Usage guidelines

Show the DNS related configuration information.

Examples

```
DES-7200# show hosts
Name servers are:
192.168.5.134 static

Host                          type               Address
TTL(sec)
switch           static      192.168.5.243          ---
www.DES-7200.com      dynamic            192.168.5.123
126
```

Related commands

Command	Description
ip host	Configure the host name and IP address mapping by manual.
ipv6 host	Configure teh host name and IPv6 address mapping by manual.
ip name-server	Configure the DNS server.

12 FTP Server Configuration Commands

12.1 Configuration Related Commands

12.1.1 debug ftp server

Use this command to enable outputting the debugging messages in the FTP server. Use the **no** form of this command to disable this function.

debug ftpserver

no debug ftpserver

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Privileged user mode.

Usage guidelines

Use this command to display the detailed debugging information during FTP server operation.

Examples

The following example shows how to enable outputting the debugging messages in the FTP Server:

```
DES-7200# debug ftpserver
FTPSRV_DEBUG:(RECV)   SYST
FTPSRV_DEBUG:(REPLY)  215 DNOS Type: L8
FTPSRV_DEBUG:(RECV)   PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY)  200 PORT Command okay.
```

The following example shows how to disable outputting the debugging messages in the FTP Server:

```
DES-7200# no debug ftpserver
```

Platform description N/A

12.1.2 ftp-server enable

Use this command to enable the FTP server. Use the **no** form of this command to disable the FTP server.

ftp-server enable

no ftp-server enable

Parameter description

Parameter	Description
-	-

Default Settings Disabled

Command mode Global configuration mode.

Usage guidelines

This command is used to enable the FTP server to connect the FTP client to upload/download the files.

Caution

To enable the FTP client to access to the FTP server files, this command shall be co-used with the **ftp-server topdir** command.

Examples

The following example shows how to enable the FTP Server and make the FTP client access to the syslog content only:

```
DES-7200(config)# ftp-server topdir /syslog
DES-7200(config)# ftp-server enable
```

The following example shows how to disable the FTP Server:

```
DES-7200(config)# no ftp-server enable
```

12.1.3 ftp-server password

Use this command to set the login password for the FTP server. Use the **no** form of this command to cancel the password configuration.

ftp-server password [*type*] *password*

no ftp-server password

Parameter description

Parameter	Description
type	Define the encryption type of the password: 0 or 7. The default type is 0. 0 indicates the password is not encrypted. 7 indicates the password is encrypted.
password	The login password for the FTP server.

Default Settings

By default, there is no password.

Command mode

Global configuration mode.

Usage guidelines

For the FTP server, the login username and the login password must be configured to verify the client connection. One password can be set at most.

The password must include the letter or number. The space in front of / behind the password is allowed, but it is ignored. While the space in the middle of the password is a part of password.

The minimum and maximum lengths of the plain-text password are 1 character and 25 characters.

The minimum and maximum lengths of the encrypted password are 4 characters and 52 characters respectively.

The encrypted password is generated by plain-text password encryption and its format must comply with the encryption specification. If the encrypted password is used for the setting, the client must use the corresponding plain-text password for the purpose of successful login.

Caution

Null password is not supported by the FTP server. Without the password configuration, the client fails to pass the identity verification of the server.

Examples

The following example shows how to set the plain-text password as *pass*:

```
DES-7200(config)# ftp-server password pass
OR:
DES-7200(config)# ftp-server password 0 pass
```

The following example shows how to set the cipher-text password as *8001*:

```
DES-7200(config)# ftp-server password 7 8001
```

The following example shows how to delete the password configuration:

```
DES-7200(config)# no ftp-server password
```

Platform description N/A

12.1.4 ftp-server topdir

Use this command to set the directory range for the FTP client to access to the FTP server files. Use the **no** form of this command to prevent the FTP client from accessing to the FTP server files.

ftp-server topdir *directory*

no ftp-server topdir

Parameter description

Parameter	Description
directory	Set the top-directory.

Default Settings By default, no top-directory is configured.

Command mode Global configuration mode.

Usage The FTP server top directory specifies the directory range

guidelines	of the files accessed by the client. Can the FTP client accesses to the files on the FTP server with the top directory correctly specified. Without this command configured, FTP client fails to access to any file or directory on the FTP server.

Examples	The following example shows how to enable the FTP Server and make the FTP client access to the syslog content only:
	`DES-7200(config)# ftp-server topdir /syslog`
	`DES-7200(config)# ftp-server enable`
	
	The following example shows how to remove the top-directory configuration:
	`DES-7200(config)# no ftp-server topdir`

Platform description	N/A

12.1.5 ftp-server timeout

Use this command to set the FTP session idle timeout. Use the **no** form of this command to restore the idle timeout to the default value（30 minutes）.

ftp-server timeout *time*

no ftp-server timeout

Parameter description

Parameter	Description
time	Set the session idle timeout, in minutes. The valid range is 1-3600.

Default Settings	Default time is 30 minutes.
Command mode	Global configuration mode.
Usage guidelines	Use this command to set the FTP session idle timeout. If the session is idle, the FTP server deems the session connection is invalid and disconnects with the user. **Caution**

	The session idle time refers to the time for the FTP session between two FTP operations.

Examples	The following example shows how to set the session idle timeout as 5m:
	`DES-7200(config)# ftp-server timeout 5`
	The following example shows how to restore the session idle timeout to the default value(30m):
	`DES-7200(config)# no ftp-server timeout`

Platform description	N/A

12.1.6 ftp-server username

Use this command to set the login username for the FTP server. Use the **no** form of this command to cancel the username configuration.

ftp-server username *username*

no ftp-server username

Parameter description

Parameter	Description
username	Set the login username.

Default Settings	By default, no username is set.
Command mode	Global configuration mode.
Usage guidelines	Use this command to set the login username for the FTP server. To log in to the FTP server, the correct username and password shall be provided. The maximum length of the username is 64 characters and the spaces are not allowed in the middle of the username. The username consists of letters, semiangle number and semiangle mark. One username can be configured for the FTP server at most. **Caution** The anonymous user login is not supported on the FTP

server. The client fails to pass the identity verification if the username is removed.

Examples

The following example shows how to set the username as *user*:

```
DES-7200(config)# ftp-server username user
```

The following example shows how to remove the username configuration:

```
DES-7200(config)# no ftp-server username
```

Platform description N/A

12.2 Showing Related Commands

12.2.1 show ftp-server

Use this command to show the status information of the FTP server.

show ftp-server

Parameter description

Parameter	Description
-	-

Default Settings N/A.

Command mode Privileged EXEC mode.

Usage guidelines

The FTP server status information includes:

- Enabled/Disabled server
- The control connection is set up or not (the related IP, Port are shown)
- The data connection is set up or not (the related IP, Port and the working mode are shown)
- The current file transmission type
- The login username and password
- The FTP server top directory
- The session idle timeout setting

Examples

The following example shows the related status information of the FTP server:

```
DES-7200# show ftp-server
ftp-server information
=====================================
enable : Y
topdir : /
timeout: 20min
username config : Y
password config : Y
type: BINARY
control connect : Y
ftp-server: ip=192.167.201.245  port=21
ftp-client: ip=192.167.201.82  port=4978
port data connect : Y
ftp-server: ip=192.167.201.245  port=22
ftp-client: ip=192.167.201.82  port=4982
passive data connect : N
```

Platform description N/A

13 TCP Configuration Commands

13.1 Configuration Related Commands

13.1.1 ip tcp path-mtu-discovery

Use this command to enable PMTU(Path Maximum Transmission Unit) discovery function for TCP in the global configuration mode. Use the **no** form of this command to disable this function.

ip tcp path-mtu-discovery [**age-timer** {*minutes* **| infinite**}]
no ip tcp path-mtu-discovery [**age-timer** {*minutes* **| infinite**}]

Parameter description

Parameter	Description
age-timer *minutes*	(Optional) Set the interval for the re-detection after the TCP discovers PMTU, in minutes. The default time is 10m. The valid range is 10-30m.
age-timer infinite	(Optional) No re-detection after the TCP discovers the PTMU.

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

Based on the RFC1191, the TCP path mtu function improves the network bandwidth utilization and data transmission when the user uses TCP to transmit the data in batch.

Enabling or disabling this function takes no effect for the existent TCP connection and is only effective for the TCP

connection to be created. This command is valid for both the IPv4 and IPv6 TCP.

According to the RFC1191, after discovering the PMTU, the TCP uses greater MSS to detect the new PMTU at some interval, which is specified by the parameter **age-timer**. If the PMTU discovered is smaller than the MSS negotiated between both ends of the TCP connection, the device will be trying to discover the greater PMTU at the specified interval untill the PMTU value reaches the MSS or the user stops using this timer. Use the parameter **age-timer infinite** to stop this timer.

Examples

The following example shows how to enable the TCP PMTU discovery function:

```
DES-7200(config)# ip tcp path-mtu-discovery
```

Related commands

Command	Description
show tcp pmtu	Show the PMTU value for the TCP connection.

13.2 Showing Related Commands

13.2.1 show tcp pmtu

Use this command to view the TCP PMTU information.

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to view the PMTU value for the TCP connection.

Examples

```
DES-7200# show tcp pmtu
```

```
No.     Local Address          Foreign Address       PMTU
[1]    2002::1.18946          2002::2.23            1440
[2]  192.168.195.212.23    192.168.195.112.13560  1440
```

The following table is the field description :

Field	Description
No.	Sequence number.
Local Address	The local address and the port number. The number after the last “.” is the port number. For example, “2002::2.23” and “192.168.195.212.23” , “23” is the port number.
Foreign Address	The remote address and the port number. The number after the last “.” is the port number. For example, “2002::2.23” and “192.168.195.212.23” , “23” is the port number.
PMTU	The PMTU value.

Related commands

Command	Description
ip tcp path-mtu-discovery	Enable the TCP PMTU discovery function.

DES-7200

Network Management Command Reference Guide

Version 10.4(3)

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 SNMP Configuration Command

1.1 Configuration Related Commands

1.1.1 no snmp-server

Use this command to disable the SNMP agent function in the global configuration mode.

no snmp-server

Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	This command disables the SNMP agent services of all versions supported on the device.
Examples	The example below disables the SNMP agent service. `DES-7200(config)# no snmp-server`

1.1.2 snmp-server chassis-id

Use this command to specify the SNMP system sequential number in the global configuration mode. The **no** form of this command is used to restore it to the initial value.

snmp-server chassis-id *text*

no snmp-server chassis-id

Parameter description

Parameter	Description
text	Text of the system sequential number, numerals or characters.

Default configuration	The default sequence number is 60FF60.
Command mode	Global configuration mode.
Usage guidelines	The SNMP system sequence number is generally the sequence number of the machine to facilitate the device identification. The sequence number can be viewed through the **show snmp** command.
Examples	The example below specifies the SNMP system sequence number as 123456: `DES-7200(config)# snmp-server chassis-id 123456`

Related commands

Command	Description
show snmp	Show the SNMP information.

1.1.3 snmp-server community

Use this command to specify the SNMP community access string in the global configuration mode. The **no** format of the command cancels the SNMP community access string.

snmp-server community *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [**ipv6** *ipv6-aclname*] [*aclnum*] [*aclname*]

no snmp-server community *string*

Parameter description

Parameter	Description
string	Community string, which is equivalent to the communication password between the NMS and the SNMP agent
view-name	Name of the view used for management
ro	Indicate that the NMS can only read the variables of the MIB.
rw	Indicate that the NMS can read and write the variables of the MIB.
aclnum	Sequence number of the ACL, which specifies the IPV4 address range of the

	NMS that are permitted to access the MIB.
aclname	Name of the ACL, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
ipv6-aclname	Name of the IPv6 ACL, which specifies the IPv6 address range of the NMS that are permitted to access the MIB
ipaddr	IP address of the NMS accessing the MIB

Default configuration All communities are read only by default.

Command mode Global configuration mode.

Usage guidelines

This command is the first important command to enable the SNMP agent function. It specifies the community attribute, range of the NMSs that can access the MIB, and more.

To disable the SNMP agent function, execute the command **no snmp-server**.

Examples

The example below restricts the access to the MIB through the access list, which allows only the NMS of the IP address 192.168.12.1 to access the MIB.

```
DES-7200(config)# access-list 2 permit 192.168.12.1
DES-7200(config)# access-list 2 deny any
DES-7200(config)# snmp-server community public ro 2
```

Related commands

Command	Description
access-list	Define the access list.

1.1.4 snmp-server contact

Use this command to specify the SNMP system contact in the global configuration mode. The **no** form of this command is used to delete the system contact.

snmp-server contact *text*

no snmp-server contact

Parameter description

Parameter	Description
text	String describing the system contact.

Default configuration N/A.

Command mode Global configuration mode.

Examples The example below specifies the SNMP system contract i-net800@i-net.com.cn:

```
DES-7200(config)# snmp-server contact
i-net800@i-net.com.cn
```

Related commands

Command	Description
show snmp-server	Check the SNMP information.
no snmp-server	Disable the SNMP agent function.

1.1.5 snmp-server enable traps

Use this command to enable the SNMP server to actively send the SNMP Trap massage to NMS when some emergent and important events occur in the global configuration mode. The **no** format of this command is used to disable the SNMP server to actively send the SNMP Trap massage to NMS.

snmp-server enable traps [snmp]

no snmp-server enable traps

Parameter description

Parameter	Description
snmp	Enable the trap notification of SNMP events.

Default configuration Disabled.

Command mode Global configuration mode.

Usage guidelines	This command must work with the global configuration command **snmp-server host** to send the SNMP Trap message.

Examples	The example below enables the SNMP server to actively send the SNMP Trap message.
	`DES-7200(config)# snmp-server enable traps snmp`
	`DES-7200(config)# snmp-server host 192.168.12.219 public snmp`

Related commands

Command	Description
snmp-server host	Specify the SNMP host to send the SNMP Trap message.

1.1.6 snmp-server group

Use this command to set the SNMP user group in the global configuration mode**.** The **no** form of this command is used to remove the user group.

snmp-server group ***groupnam****e* **{v1 | v2c | v3 {auth | noauth | priv}} [read** *readview***][write** *writeview***] [access** {[ipv6 ipv6_aclname] [*aclnum* |*aclname*] num|name}**]**

no snmp-server group *groupname* {**v1 | v2c | v3** }

Parameter description

Parameter	Description
v1,v2c,v3	SNMP version
auth	Authenticate the messages transmitted by the user group without encryption. This applies to only SNMPv3.
noauth	Neither authenticate nor encrypt the messages transmitted by the user group. This applies to only SNMPv3.
priv	Authenticate and encrypt the messages transmitted by the user group. This applies to only SNMPv3.
readview	Associate with a read-only view.
aclnum	Sequence number of the ACL in the range of 1 to 99, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which specifies the IPV4 address range of the NMS that

		are permitted to access the MIB.
	ipv6_aclname	Name of the IPv6 ACL, which specifies the IPv6 address range of the NMS that are permitted to access the MIB
	writeview	Associate with a read-write view.

Default configuration	N/A.
Command mode	Global configuration mode.
Examples	The example below sets a user group. `DES-7200(config)#` **`snmp-server group`** *`mib2user`* **`v3 priv read`** *`mib2`*

Related commands

Command	Description
show snmp group	Show the SNMP user group configuration.

1.1.7 snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message in the global configuration mode. The **no** form of this command is used to remove the specified SNMP host.

snmp-server host {*host-addr*| **ipv6** *ipv6-addr*} [**vrf** *vrfname*] [**traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]] *community-string* [**udp-port** *port-num*][*notification-type*]

no snmp-server host { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*]

Parameter description

Parameter	Description
host-addr	SNMP host address
ipv6-addr	SNMP host address(ipv6)
vrfname	Set the name of vrf forwarding table
version	SNMP version: V1, V2C or V3
auth | noauth | priv	Security level of SNMPv3 users

community-string	Community string or username (SNMPv3 version)
port-num	Port of the SNMP host
notification-type	The type of the SNMP trap message sent actively, such as **snmp**.

Default configuration

By default, no SNMP host is specified.

If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.

Command mode

Global configuration mode.

Usage guidelines

This command must work with the **snmp-server enable traps** command in the global configuration mode to actively send the SNMP trap messages to NMS.

It is possible to configure multiple SNMP hosts to receive the SNMP Trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages have to be configured.

Examples

The example below specifies an SNMP host to receive the SNMP event trap:

```
DES-7200(config)# snmp-server host 192.168.12.219 public snmp
```

Related commands

Command	Description
snmp-server enable traps	Enable to send the SNMP trap message.

1.1.8 snmp-server location

Use this command to set the SNMP system location information in the global configuration mode. The **no** form of this command is used to remove the specified SNMP system location information.

snmp-server location *text*

no snmp-server location

Parameter description

Parameter	Description
text	String describing the system

Default configuration Null

Command mode Global configuration mode.

Examples The example below specifies the system information:

```
DES-7200(config)# snmp-server location
start-technology-city 4F of A Buliding
```

Related commands

Command	Description
snmp-server contact	Specify the system contact information.

1.1.9 snmp-server packetsize

Use this command to specify the maximum size of the SNMP packet in the global configuration mode. The **no** form of this command is used to restore it to the default value.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter description

Parameter	Description
byte-count	Packet size in the range of 484 to 17876 bytes

Default configuration 1472 bytes.

Command mode Global configuration mode.

Examples The example below specifies the maximum SNMP packet size as 1,492 bytes:

```
DES-7200(config)# snmp-server packetsize 1492
```

Related commands

Command	Description
snmp-server queue-length	Specify the length of the SNMP trap message queue.

1.1.10 snmp-server queue-length

Use this command to specify the length of the SNMP trap message queue in the global configuration mode.

snmp-server queue-length *length*

Parameter description

Parameter	Description
length	**Queue length in the range of 1 to 1000**

Default configuration

10.

Command mode

Global configuration mode.

Usage guidelines

The SNMP trap message queue is used to store the SNMP trap messages. This command can be used to adjust the size of the SNMP trap message queue to control the speed to sending the SNMP trap messages.

The maximum speed to send messages is 4 messages per second.

Examples

The example below specifies the speed to send the trap message to 4 messages per second:

```
DES-7200(config)# snmp-server queue-length 4
```

Related commands

Command	Description
snmp-server packetsize	Specify the maximum size of the SNMP packet.

1.1.11 snmp-server system-shutdown

Use this command to enable the SNMP system restart notification function in the global configuration mode. The **no** form of this command is used to disable the SNMP system notification function.

snmp-server system-shutdown

no snmp-server system-shutdown

Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	This command is used to enable the SNMP system restart notification function. The DES-7200 sends the SNMP trap messages to the NMS to notify the system pending before the device is reloaded or rebooted.
Examples	The example below enables the SNMP system restart notification function: `DES-7200(config)# snmp-server system-shutdown`

1.1.12 snmp-server trap-source

Use this command to specify the source of the SNMP trap message in the global configuration mode. The **no** form of this command is used to restore it to the default value.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter description

Parameter	Description
interface	Interface to be used as the source of the SNMP trap message

Default configuration	The IP address of the interface where the NMP message is sent from is just the source address.
Command mode	Global configuration mode.

Usage guidelines

By default, the IP address of the interface where the NMP message is sent from is just the source address. For easy management and identification, this command can be used to fix a local IP address as the SNMP source address.

Examples

The example below specifies the IP address of Ethernet interface 0 as the source of the SNMP trap message:

```
DES-7200(config)# snmp-server trap-source fastethernet 0
```

Related commands

Command	Description
snmp-server enable traps	Enable the sending of the SNMP trap message.
snmp-server host	Specify the NMS host to send the SNMP trap message.

1.1.13 snmp-server trap-timeout

Use this command to define the retransmission timout time of the SNMP trap message in the global configuration mode. The **no** form of this command is used to restore it to the default value.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter description

Parameter	Description
seconds	Timeout (in seconds) of retransmit the SNMP trap message

Default configuration

30s.

Command mode

Global configuration mode.

Examples

The example below specifies the timeout period as 60 seconds.

```
DES-7200(config)# snmp-server trap-timeout 60
```

Related

Command	Description

snmp-server queue-length	Specify the length of the SNMP trap message queue.
snmp-server host	Specify the NMS host to send the SNMP trap message.

1.1.14 snmp-server user

Use this command to set the SNMP name in the global configuration mode**.** The **no** form of this command is used to delete the user.

snmp-server user *username groupname* {**v1 | v2c | v3** [**encrypted**] [**auth** {**md5 | sha**} *auth-password*] [**priv des56** *priv-password*]} [**access** {[ipv6 ipv6_aclname][acl*num* | acl*name*}]]

no snmp-server user *username groupname* {**v1 | v2c | v3** }

Parameter description

Parameter	Description
username	User name
groupname	Group name of the user.
v1 | v2c | v3	SNMP version. But only SNMPv3 supports the following security parameters.
encrypted	Input the password in cipher text mode. In cipher text mode, input continuous HEX alphanumeric characters. Note that the authentication password of MD5 has a length of 16 characters, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can only be used by the local SNMP engine on the switch.
auth	Specify whether to use the authentication.
auth-password	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
priv	Encryption mode. **des56** refers to 56-bit DES encryption protocol. *priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.

md5	Enable the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
aclnumber	Sequence number of the ACL in the range of 1 to 99, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 ACL, which specifies the IPv6 address range of the NMS that are permitted to access the MIB

Default configuration N/A.

Command mode Global configuration mode.

Examples The example below configures an SNMPv3 user with MD5 authentication and DES encryption:

```
DES-7200(config)# snmp-server user user-2 mib2user v3
auth md5 authpassstr priv des56 despassstr
```

Related commands

Command	Description
show snmp user	Show the SNMP user configuration.

1.1.15 snmp-server view

Use this command to set a SNMP view in the global configuration mode**.** The **no** form of this command is sued to delete the view.

snmp-server view *view-name* **oid-tree** {**include | exclude**}

no snmp-server view *view-name* [***oid-tree***]

Parameter description

Parameter	Description
view-name	View name
oid-tree	Specify the MIB object to associate with the view.

	include	Include the sub trees of the MIB object in the view.
	exclude	Exclude the sub trees of the MIB object from the view.

Default configuration	By default, a default view is set to access all MIB objects.
Command mode	Global configuration mode.
Examples	The example below sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1). `DES-7200(config)# snmp-server view mib2 1.3.6.1 include`

Related commands	**Command**	**Description**
	show snmp view	Show the view configuration.

1.1.16 snmp trap link-status

For this command, please refer to the *INTF-CREF.doc*

Parameter description	N/A
Default configuration	Please refer to the *INTF-CREF.doc.*
Command mode	Please refer to the *INTF-CREF.doc.*
Examples	Please refer to the *INTF-CREF.doc*

1.2 Showing Related Command

1.2.1 show snmp

Use this comand to show the SNMP information in the privileged mode.

show snmp [**mib | user | view | group | host**]

Command mode	Privileged mode.
Usage guidelines	**show snmp**: Show the SNMP information. **show snmp mib**: Show the SNMP MIBs supported in the system. **show snmp user**: Show the SNMP user information. **show snmp view**: Show the SNMP view information. **show snmp group**: Show the SNMP user group information. **Show snmp host**: show the configuration set by users.

Examples	The example below shows the SNMP information:
	`DES-7200# show snmp`
	`Chassis: 60FF60`
	`0 SNMP packets input`
	`0 Bad SNMP version errors`
	`0 Unknown community name`
	`0 Illegal operation for community name supplied`
	`0 Encoding errors`
	`0 Number of requested variables`
	`0 Number of altered variables`
	`0 Get-request PDUs`
	`0 Get-next PDUs`
	`0 Set-request PDUs`
	`0 SNMP packets output`
	`0 Too big errors (Maximum packet size 1472)`
	`0 No such name errors`
	`0 Bad values errors`
	`0 General errors`
	`0 Response PDUs`
	`0 Trap PDUs`
	`SNMP global trap: disabled`
	`SNMP logging: disabled`
	`SNMP agent: enabled`

Related commands

Command	Description
snmp-server chassis-id	Specify the SNMP system sequence number.

2 RMON Configuration commands

2.1 Configuration Related Commands

2.1.1 rmon alarm

Use this command to monitor a MIB variable. The **no** form of this command cancels the logging.

rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]

no rmon alarm *number*

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	The DES-7200 allows you to modify the configured history information of the Ethernet network, including **variable, absolute/delta, owner, rising-threadhold/falling-threadhold**, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.
Examples	The example below monitors the MIB variable instance ifInNUcastPkts.6. `DES-7200(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-threshold 10 1 owner zhangsan`
Related	**Command** / **Description**

	rmon event *number* [**log**] [**trap** *community*] **description** *string* [**owner** *owner-string*]	Add an event definition.

2.1.2 rmon collection history

Use this command to log the history of an Ethernet interface. The **no** form of this command cancels the logging.

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Default N/A.

Command mode Interface configuration mode.

Usage guidelines The DES-7200 allows you to modify the configured history information of the Ethernet network, including **owner, buckets**, and **interval**. However, the modification does not take effect immediately until the system records history at the next time.

Examples The example below Logs the history of Ethernet port 1.

```
DES-7200(config)# interface fast-Ethernet 0/1
DES-7200(config-if)# rmon collection history  1 zhansan
buckets 10 interval 10
```

Related commands

Command	Description
rmon collection stats *index* [**owner** *owner-name*]	Add a statistical entry.

2.1.3 rmon collection stats

Use this command to monitor an Ethernet interface. The **no** form of this command remove the configuration.

rmon collection stats *index* [**owner** *owner-string*]

no rmon collection stats *index*

Default N/A.

Command mode	Interface configuration mode.
Usage guidelines	N/A.

Examples	The example below enables monitoring the statistics of Ethernet port 1.
	`DES-7200(config)# interface fast-Ethernet 0/1`
	`DES-7200(config-if)# rmon collection stats 1 zhansan`

Related commands

Command	Description
rmon collection history *index* [**owner** *owner-name*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history control entry.

2.1.4 rmon event

Use this command to define an event. The **no** form of this command cancels the logging.

rmon event *number* [**log**] [**trap** *community*] [*description-string*] [**description** *description-string*] [**owner** *owner-name*]

no rmon alarm *number*

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	N/A.
Examples	The example below defines the event actions: log event and send trap message. `DES-7200(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much " owner zhangsan`

Related

Command	Description

	rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry.

2.2 Showing Related Commands

2.2.1 show rmon alarm

Use this command to show the rmon alarm table.

show rmon alarm

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The example below shows the rmon alarm table.
	`DES-7200# show rmon alarm`
	`rmon alarm table:`
	`index: 10,`
	`interval: 30,`
	`oid = 1.3.6.1.2.1.2.2.1.12.6`
	`sampleType: 2,`
	`alarmValue: 0,`
	`startupAlarm: 3,`
	`risingThreshold: 20,`
	`fallingThreshold: 10,`
	`risingEventIndex: 1,`
	`fallingEventIndex: 1,`
	`owner: zhangesan,`
	`stats: 1,`

Related	**Command**	**Description**

	rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry.

2.2.2 show rmon event

Use this command to show the event information.

show rmon event

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The example below shows the event information.
	`DES-7200# show rmon event`
	`rmon event table:`
	`index = 1`
	`description = ifInNUcastPkts`
	`type = 4`
	`community = rmon`
	`lastTimeSent = 0 d:0 h:0 m:0 s`
	`owner = zhangsan`
	`status = 1`

Related commands	**Command**	**Description**
	rmon event *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	Add an event entry.

2.2.3 show rmon history

Use this command to show the history information.

show rmon history

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples

The example below shows the history information.

```
DES-7200#  show rmon history
rmon history control table:
                index = 1
                interface = FastEthernet 0/1
                bucketsRequested = 10
                bucketsGranted = 10
                interval = 1800
                owner = zhangsan
                stats = 1

rmon history table:
                index = 1
                sampleIndex = 198
                intervalStart = 0d:14h:0m:47s
                dropEvents = 0
                octets = 67988
                pkts = 726
                broadcastPkts = 502
                multiPkts = 189
                crcAllignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
```

	Command	Description
Related commands	**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history control entry.

2.2.4 show rmon statistics

Use this command to show the statistics.

show rmon statictics

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.
Examples	The example below shows the statistics.

```
DES-7200#  show rmon statistics
ether statistic table:
                index = 1
                interface = FastEthernet 0/1
                owner = zhangsan
                status = 0
                dropEvents = 0
                octets = 1884085
                pkts = 3096
                broadcastPkts = 161
                multiPkts = 97
                crcAllignErrors = 0
                underSizePkts = 0
                overSizePkts = 1200
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 128
                packets65To127Octets = 336
```

```
packets128To255Octets = 229
packets256To511Octets = 3
packets512To1023Octets = 0
packets1024To1518Octets = 1200
```

Related commands

Command	Description
rmon collection stats *index* [**owner** *owner-string*]	Add a statistical entry.

3 NTP Configuration Commands

3.1 NTP Configuring Related Commands

3.1.1 no ntp

Use this command to disable the **ntp** synchronization service with the time server and clear all configuration information of **ntp**.

no ntp

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	By default, the NTP function is disabled. However, once the NTP server or the NTP security identificaiton mechanism is configured, the NTP function will be enabled.
Examples	The configuration example below disables the NTP service. `DES-7200(config)#no ntp`

Related commands

Command	Description
ntp server	Specify a NTP server.

3.1.2 ntp access-group

Use this command to configure the access control priority of the ntp service. Use the **no** form of this command to cancel the access control priority.

ntp access-group {peer | serve | serve-only | query-only} *access-list-number* | *access-list-name*

no ntp access-group {peer | serve | serve-only | query-only} *access-list-number* | *access-list-name*

Parameter description

Parameter	Description
peer	Not only allow to request for the time of and control the local NTP service, but also allow the time synchronization of the local and the peer.
serve	Allow to request for the time of and control the local NTP service only, the time synchronization of the local and the peer is not allowed.
serve-only	Allow to request for the time of local NTP service only.
query-only	Allow to control and search for the local NTP service.
access-list-number	The IP access control list number, in the range of 1-99 and 1300-1999.
access-list-name	The IP access control list name.

Default

No NTP access control rule has been configured by default.

Command mode

Global configuration mode.

Usage guidelines

Use this command to configure the access control priority of the ntp service. NTP services access control function provides a minimal security measures (more secure way is to use the NTP authentication mechanism).

When an access request arrives, NTP service matches the rules in accordance with the sequence from the smallest to the largest to access restriction, and the first matched rule shall prevail. The matching order is peer, serve, serve-only, query-only.

Caution:

Control query function is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

If you do not configure any access control rules, then all accesses are allowed. However, once the access control rules are configured, only the rule that allows access can be carried out.

Examples

The following example shows how to allow the peer device in acl1 to control the query, request for and synchronize the time with the local device; and limit the peer device in acl2 to request the time for the local device:

```
DES-7200(config)# ntp access-group peer 1

DES-7200(config)# ntp access-group serve-only 2
```

Related commands

Command	Description
ip access-list	Create the IP access control list.

3.1.3 ntp authenticate

Use this command to enable NTP authentication globally.

ntp authenticate

no ntp authenticate

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	If the global security identification mechanism is not used, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the security identification mechanism and configure other keys globally. The authentication standard is the trusted key specified by **ntp authentication-key** and **ntp trusted-key**.

Examples	After an authentication key is configured and specified as the global trusted key, enable the authentication mechanism.
	`DES-7200(config)#ntp authentication-key 6 md5 wooooop`
	`DES-7200(config)#ntp trusted-key 6`
	`DES-7200(config)#ntp authenticate`

Related commands

Command	Description
ntp authentication-key	Set the global authentication key.
ntp trusted-key	Configure the global trusted key.

3.1.4 ntp authentication-key

Use this command to configure a global NTP authentication key for the NTP server.

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

no ntp authentication-key *key-id*

Parameter description

Parameter	Description
key-id	Key ID
key-string	Key string
enc-type	(Optional) Whether this key is encrypted, where, 0 indicates the key is

		not encrypted, 7 indicates the key is encrypted simply.

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	Configure the global authentication key and adopt **md5** for encryption. Each key presents the unique *key-id* identification. Customers can use the **ntp trusted-key** to set the key of *key-id as* the global trusted key. The upeer limit of the keys is 1024. However, each server can only support one key.
Examples	The following example configures an authentication key with ID 6. `DES-7200(config)ntp authentication-key 6 md5 wooooop`

Related commands

Command	Description
ntp authenticate	Enable the global security identification mechanism.
ntp trusted-key	Configure the global trusted key.
ntp server	Specify a NTP server.

3.1.5 ntp disable

Use this command to disable the function of receiving the NTP message on the interface.

ntp disable

Parameter description	N/A.
Default	The NTP message is received on the interface, by default.
Command mode	Interface configuration mode.

Usage guidelines	The NTP message received on any interface can be provided to the client to carry out the clock adjustment. The function can be set to shield the NTP message received from the corresponding interface. Note: The interface that is configured with this command can receive and send IP packets. No this command is configured on other interfaces.
Examples	The configuration example below disables the function of receiving the NTP message on the interface. `DES-7200(config)#no ntp disable`

3.1.6 ntp master

Use this command to configure the local time as the NTP master(the local time reference source is reliable), providing the synchronizing time for other devices. Use the **no** form of this command to cancel the NTP master settings.

ntp master [*stratum*]

no ntp master

Parameter description

Parameter	Description
stratum	Specify the stratum where the local time is, in the range of 1-15. The defaut stratum is 8.

Default	No NTP master is configured, by default.
Command mode	Global configuration mode.

In general, the local system synchronizes the time from the external time source directly or indirectly. However, if the time synchronization of local system fails for the network connection trouble, ect, use the command to set the reliable reference source of the local time, providing the synchronized time for other devices.

Once set, the system time can not be synchronized to the time source with higher starum.

Usage guidelines

Caution:

Using this command to set the local time as the master (in particular, specify a lower starum value), is likely to be covered by the effective clock source. If multiple devices in the same network use this command, the time synchronization instability may occur due to the time difference between the devices.

In addition, before using this command, if the system has never been synchronized with an external clock source, it is necessary to manually calibrate the system clock to prevent too much bias.

Examples

The configuration example below configures the reliable local time reference source and set the time stratum 12:

```
DES-7200(config)# ntp master 12
```

3.1.7 ntp server

Use this command to specify a NTP server for the NTP client.

ntp server *ip-addr* [**version** *version*] [**source** *if-name*] [**key** *keyid*][**prefer**]

no ntp server *ip-addr*

Parameter description

Parameter	Description
ip-addr	Set the IP address of the NTP server.
version	(Optional) Specify the version (1-3) of NTP, NTPv3 by default.
if-name	(Optional) Specify the source interface from which the NTP message is sent (L3 interface).
keyid	(Optional) Specify the encryption key

	adopted when communication with the corresponding server.
prefer	(Optional) Specify the corresponding server as the prefer server.

Default No NTP server is configured, by default.

Command mode Global configuration mode.

Usage guidelines

At present, our system only support clients other than servers, and the upeer limit of supported synchronous servers are 20.

To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server.

In the same condition (for instance, precision), the prefer clock is used for synchronization.

It should be noted that the configured interface is that configured with the IP address and can communicate with the corresponding NTP server when you configure the source interface of the NTP message.

Examples

The configuration example below configures the equipment in the network as NTP server.

For IPv4: `DES-7200(config)# ntp server 192.168.210.222`

For IPv6: `DES-7200(config)# ntp server 10::2`

Related commands

Command	Description
no ntp	Disable the NTP service function.

3.1.8 ntp synchronize

Use this command to synchronize the realtime.

ntp synchronize

no ntp synchronize

Parameter description	N/A.
Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	8 consecutive packets are synchronized for the first synchronization of NTP and each server. Then the synchronization occurs every one minute. This command is used to complete the instant synchronization during the interval of auto-sync.
Examples	The following example synchronizes the NTP realtime. `DES-7200(config)#ntp synchronize`

Related commands

Command	Description
ntp server	Specify a NTP server.

Platform description	Supported by parts of products.

3.1.9 ntp trusted-key

Use this command to set a key at the global trusted key.

ntp trusted-key *key-id*

no ntp trusted-key *key-id*

Parameter description

Parameter	Description
key-id	Global trusted key ID

Default	N/A.
Command mode	Global configuration mode.

Usage guidelines	The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

Examples	The following configures an authentication key and sets it as the corresponding server trusted key.
	`DES-7200(config)#ntp authentication-key 6 md5 wooooop`
	`DES-7200(config)#ntp trusted-key 6`
	`DES-7200(config)#ntp server 192.168.210.222 key 6`

Related commands

Command	Description
ntp authenticate	Enable the security authentication mechanism.
ntp authentication-key	Set the NTP authentication key.
ntp server	Specify a NTP server.

3.1.10 ntp update-calendar

Use this command to update the calendar for the NTP client using the synchronization time of the external time source. Use the **no** form of this command to disable the update-calendar function

ntp update-calendar

no ntp update-calendar

Parameter description	N/A.
Default	By default, update the calendar periodically is not configured.
Command mode	Global configuration mode.
Usage guidelines	By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

Examples	The following configures the NTP update calendar periodically. `DES-7200(config)# ntp update-calendar`

3.2 Showing and Monitoring Commands

3.2.1 debug ntp

Use this command to show the NTP debugging information.

debug ntp

no debug ntp

Parameter description	N/A.
Default	Disabled.
Command mode	Privileged mode.
Usage guidelines	To carry out the NTP function debugging, output necessary debugging information to implement the failure diagnosis and troubleshooting by this command.
Examples	The example below enables the NTP debugging switch. `DES-7200(config)#debug ntp`

3.2.2 show ntp status

Use this command to show the NTP information.

show ntp status

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.

Usage guidelines	If the NTP service of the system is enabled, show current NTP information. This command will not print any information before the synchronization server is added for the first time.
Examples	The example below shows the NTP information of current system. `DES-7200(config)#show ntp status`

4 SNTP Configuration Commands

4.1 Configuring Related Commands

4.1.1 sntp enable

Use this command to enable the SNTP function. Use the **no** form of this command to restore the default value.

[no] sntp enable

Default configuration	Disabled
Command mode	Global configuration mode.
Usage guidelines	This command shows the parameters of SNTP.
Examples	`DES-7200(config)# sntp enable`

Related commands

Command	Description
show sntp	Show the SNTP configuration.
clock update-calendar	Synchronize the software clock with the hardware clock.
clock set	Set the software clock.

Platform description	N/A

4.1.2 sntp interval

Use this command to set the interval for the SNTP Client to synchronize its clock with the NTP/SNTP Server.

sntp interva *seconds*

no sntp interval

Parameter description

Parameter	Description
seconds	Synchronization interval in 60 to 65535 seconds

Default configuration

1800s

Command mode

Global configuration mode.

Usage guidelines

The **show sntp** command shows the parameters of SNTP.

Caution

Note that the set interval will not take effect immediately. To this end, execute the **sntp enable** command after setting the interval.

Examples

```
DES-7200(config)# sntp interval 3600
```

Related commands

Command	Description
sntp enable	Enable SNTP.
show sntp	Show the SNTP configuration.
clock update-calendar	Synchronizes the software clock with the hardware clock.

Platform description

N/A

4.1.3 sntp server

Use this command to set the SNTP server. Since the SNTP protocol is completely compatible with the NTP protocol, you can configure the SNTP server as the public NTP server on the Internet.

sntp server *ip-address*

no sntp server

Parameter description

Parameter	Description
ip-address	The IP address of the NTP/SNTP server.

Default configuration No NTP/SNTP server is configured.

Command mode Global configuration mode.

Usage guidelines The **show sntp** command shows the parameters of SNTP.

Examples

```
DES-7200(config)# sntp server 192.168.4.12
```

Related commands

Command	Description
show sntp	Show the SNTP configuration.
sntp enable	Enable SNTP.

Platform description N/A

4.2 Showing Related Command

4.2.1 show sntp

Use this command to show the parameters of SNTP.

show sntp

Command mode

Privileged mode.

Usage guidelines

This command shows the parameters of SNTP.

Examples

```
DES-7200# show  sntp
SNTP state          : Enable
SNTP server         : 192.168.4.12
SNTP sync interval   : 60
Time zone            : +8
```

Related commands

Command	Description
sntp enable	Enable SNTP.
show sntp	Show the SNTP configuration.

Platform description

N/A

5 SPAN Configuration Commands

5.1 Configuration Related Commands

5.1.1 monitor session

Use this command to create a SPAN session and specify the destination port (monitoring port) and source port (monitored port). The **no** form of the command is used to delete the session or delete the source port or destination port separately.

monitor session *session_number* **{source interface** *interface-id* **[both | rx | tx] | destination interface** *interface-id* **{ encapsulation | switch } | mac {source** *mac-addr***| destination** *mac-addr* **} [both | rx | tx]} [acl** *name***]**

no monitor session *session_number* **[source interface** *interface-id* **[both | rx | tx] | destination interface** *interface-id* **{ encapsulation | switch }] | mac {source** *mac-addr***| destination** *mac-addr* **} [both | rx | tx] [acl** *name***]**

no monitor session all

Parameter description

Parameter	Description
session_number	SPAN session number
source interface *interface-id*	Specify the source port. *interface-id*: interface ID, which can be physical interface, not SVI. DES-7200 series support AP.
destination interface *interface-id*	Specify the destination port. *interface-id*: interface ID, which can be physical interface, not SVI.
mac source mac-addr	The source MAC address of the mirrored frame.
mac destination mac-addr	The destination MAC address of the mirrored frame.
both acl name	Monitor the inbounding and

	outbounding frames simultaneously. **acl** *name/id* of monitored flow
rx	Monitor only the inbounding frames.
tx	Monitor only the outbounding frames.
all	Delete all sessions.
encapsulation	Support the encapsulation function for the monitored port. Once this function is enabled, the tag of the mirrored frame is peeled off forcibly. This function is disabled by default.
switch	Enable switching on the mirroring destination port. It is disabled by default.

Command mode

Global configuration mode.

Usage guidelines

Both switch port and routed port can be configured as the source port or destination port. The SPAN session has no effect on the normal operation of the equipment. You can configure a SPAN session on disabled ports. However, the SPAN does not work unless you enable the source and destination ports.

A port can not be configured as the source port and the destination port at the same time.

You will remove the whole session if you do not specify the source port or the destination port.

Use **show monitor** to display SPAN session status.

Note: 1). session 1 supports global port mirroring crossing line cards. To configure the SPAN crossing the line cards, only the session 1 can be used.

Examples

The example below describes how to create a SPAN session: session 1: If this session is set previously, clear the configuration of current session 1 firstly, and then set the frame mapping of port 1 to port 8.

```
DES-7200(config)# no monitor session 1
DES-7200(config)# monitor session 1 source interface
gigabitEthernet 1/1 both
DES-7200(config)# monitor session 1 destination
interface gigabitEthernet 1/8
```

Related commands

Command	Description
show monitor	Use this command to display the SPAN configurations.

Platform description

- DES-7200 series switches support up to 128 sessions.
- DES-7200 series do not support the source/destination MAC-based frame mirror.

5.1.2 show monitor

Use this command to display the SPAN configurations.

show monitor [**session** *session_number*]

Default configuration

All SPAN sessions are displayed by default.

Parameter description

Parameter	Description
session *session_number*	SPAN session number.

Command mode

Privileged mode.

Usage guidelines

N/A.

Examples

This example shows how to use **show monitor** to display SPAN session 1**:**

```
DES-7200# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

Related

Command	Description

	monitor session	Specify a SPAN session and the destination port (mirroring port) and the source port (mirrored port).

6 RSPAN Configuration Commands

6.1 Configuration Related Commands

6.1.1 monitor session

Use this command to set RSPAN session.

Set mirror device attribute:

monitor session *session_num* {**remote-destination** | **remote-source**}

Set destination mirror:

monitor session *session-num* **destination remote vlan** *vlan-id* **interface** *interface-name* [**switch**]

Set remote source mirror:

monitor session *session-num* **source interface** *interface-id* [**rx** | **tx** | **both**]

Set mirror reflector port:

monitor session *session-num* **destination remote vlan** *vlan-id* **reflector-port interface** *interface-name* [**switch**]

Parameter description

Parameter	Description
session-num	Session number.
vlan-id	Remote span vlan id.
interface-id	Interface number .

Command mode

Global configuration mode.

Usage guidelines

Key in **end** or **Ctrl+C** to return to the privileged mode.

Key in **exit** to return to the global configuration mode.

Examples

The following example configures the source switch:

```
DES-7200(config)# monitor session 2 remote-source
DES-7200(config)# monitor session 2 source interface gigabitEthernet 1/2
DES-7200(config)# monitor session 2 destination remote vlan 7 interface gigabitEthernet 1/3 switch
DES-7200(config)# monitor session 2 destination remote vlan 7 reflector-port interface gigabitEthernet 1/1 switch
```

The following example configures the destination switch:

```
DES-7200(config)# monitor session 2 remote-destination
DES-7200(config)# monitor session 2 destination remote vlan 7 interface gigabitEthernet 1/1 switch
```

Related commands

Command	Description
show monitor	Show monitor session information.

Platform description

The reflector-port keyword is unnecessary for the products that do not support the reflector port.

6.1.2 remote-span

Use this command to set **RSPAN VLAN**.

[**no**] **remote-span**

Parameter description

N/A .

Command mode

VLAN configuration mode.

Usage guidelines

Key in **end** or **Ctrl+C** to return to the privileged mode.

Key in **exit** to return to the global configuration mode.

Examples

```
DES-7200(config)# vlan 5
DES-7200(config-vlan)# remote-span
```

Related commands	

Command	Description
show vlan	Show VLAN information.

Platform description	-

DES-7200

IP Routing Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 Protocol-independent Commands

1.1 Configuration Related Commands

1.1.1 dampening

Use this command to enable the ip event dampening function on the interface. Use the **no** form of this command to disable this function.

dampening [*half-life-period* **[***reuse-threshold suppress-threshold max-suppress* **[restart [***restart-penalty***]]]]**

no dampening

Parameter description

Parameter	Description
half-life-period	Configure the half-life period of suppression penalty, in the range of 1-30. The default value is 5s.
reuse-threshold	Configure the penalty threshold to unsuppress the interface, in the range of 1-20000. The default value is 1000.
suppress-threshold	Configure the penalty threshold to suppress the interface, in the range of 1-20000. The default value is 2000.
max-suppress	Configure the maximum suppress time, in the range of 1-255. The default value is 4 times of the half-life-period.
restart	Activate the restart penalty.
restart-penalty	Configure the default penalty value on the interface, in the range of 1-20000. The default value is 2000.

Default	Disabled
Command mode	Layer-3 interface configuration mode.

Usage guidelines	This function will influence the modules of the directly-connected/host route, static route, dynamic route and VRRP. If one interface meets the configuration condition of this command, which is in the suppression status, the above influenced modules consider the status of this interface as DOWN, so as to delete the corresponding route and not transcieve the data packets on this interface.
	Re-configuring the dampening command on the interface that has been configured this command makes all dampening information on this interface cleared. However, the interface flapping times will be remained unless use the **clear counters** command to clear the statistical information of the interface.
	Too small max-suppress configured may cause the maximum penalty value obtained from the calculation smaller than the suppression threshold to make this interface will not be suppressed forever. Therefore, it belongs to the erroneous configuration. In this case, the following message will prompt for the configuration error:
	`% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time`
	Besides, when configuring this command, it will prompt the following message as well if the system memory is not enough to save this configuration:
	`% No memory, configure dampening fail!`
	For the interface layer switching of the switches (Layer-3 interface to the Layer-2 interface), for example, if one routed port is switched to the switch port, the dampening command configured on this interface will be removed.
	Note: For routers, this function can be configured on the master interface only. This function takes effect for all sub-interfaces of the master interface with this command configured, but this command cannot be configured on the sub-interface directly. This command cannot be configured on the virtual template.

Examples

The following example enables the event

```
DES-7200(config)# interface FastEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# dampening 30 1500 10000 120
```

Related commands

Command	Description
clear counters	Clear the interface counters.
show dampening interface	Show the statistical information of the ip event dampening function on all interfaces.
show interface dampening	Show the detailed information of the ip event dampening function on all interfaces.

1.1.2 distribute-list in

Use **distribute-list in** to control the route update processing in order to filter routes. Use the **no** form of this command to remove the setting.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes permitted in the access list can be received.
prefix *prefix-list-name*	Use the prefix list to filter routes.
gateway *prefix-list-name*	Use the prefix list to filter the sources of the routes.
interface-type interface-number	(Optional) Interface that the distribution list is applied to.

Default configuration

No distribution list is defined.

Command

Routing process configuration mode.

mode	
Usage guidelines	To deny some specified routes, you can configure the route distribution list to process all the received route update messages. This command does not apply to the OSPF routing protocol, because the OSPF receives the link state messages instead of specific routes. If no interface is specified, the route update messages received by all the interfaces will be processed.

Examples	The following example allows Fastethernet 0/0 to receive the routes beginning with 172.16 in RIP.
	`router rip`
	`network 200.168.23.0`
	`distribute-list 10 in fastethernet 0/0`
	`no auto-summary`
	`!`
	`access-list 10 permit 172.16.0.0 0.0.255.255`

Related commands

Command	Description
access-list	Set the access list.
prefix-list	Set the prefix list.

1.1.3 distribute-list out

Use **distribute-list out** to control the route update for the purpose of route filtering. Use the **no** form of this command to remove the setting.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes permitted in the access list can be transmitted.
prefix *prefix-list-name*	Use the prefix list to filter routes.
interface	(Optional) Interface that the distribution list is applied to.
protocol	(Optional) The routes of the specified routing protocol are redistributed.

Default configuration	None.
Command mode	Routing process configuration mode.
Usage guidelines	If no optional parameter is used in this command, the route update applies to all the interfaces. If the interface option is used, the route update applies to only the interface. If other routing process parameters are used, the routes of the specified routing process are filtered for redistribution. The route update in the OSPF routing process only applies to the external routes of the OSPF AS, and no interface shall be specified.

Examples	The following example advertises 192.168.12.0/24 in RIP.
	`router rip`
	`network 200.4.4.0`
	`network 192.168.12.0`
	`distribute-list 10 out`
	`version 2`
	`!`
	`access-list 10 permit 192.168.12.0`

Related commands

Command	Description
access-list	Define the access list.
prefix-list	Define the prefix list.
redistribute	Redistribute routes.

1.1.4 ip community-list

Use this command to define a community list and control access to it. Use the **no** form of this command to remove the setting.

ip community-list {[**standard | expanded**] *community-list-name* | *community-number* } {**permit** | **deny**} [*community-number*]

no ip community-list {**standard | expanded**} {*community-list-name* | *community-number*}

Parameter description

Parameter	Description
community-list-name	Name of the community list of no more than 32 characters
standard	Set a standard community list numbered in 1 to 99.
expanded	Set an expanded community list numbered over 100.
permit	Permit access to the community list.
deny	Deny access to the community list.
community-number	Community number in the form of AA:NN(AS number/2-byte numerical) in the range of 1 to 255 characters. It may also be one of the following value: Internet: Indicates the Internet community. All paths belong to this community. no-export: Indicates that this path will not be advertised to any EBGP peers. no-advertise:Indicates that this path will not be advertised to any BGP peers. local-as:Indicates that this path will not be advertised to out of the AS. When AS confederation is configured, this path will not be advertised to other ASs or sub-ASs.

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

This command is used to define the community list for BGP.

Examples	DES-7200(config)# **ip community-list standard 1 deny** *100.20.200.20* DES-7200(config)# **ip community-list standard 1 permit internet**

Related commands	Command	Description
	match community	Match the community list.
	set community-list delete	Remove the community value of the BGP path according to the community list.
	show ip community-list	Show the community list information.

1.1.5 ip default-network

Use this command to configure the default network globally. Use the **no** form of this command to remove the setting.

ip default-network *network*

no ip default-network *network*

Parameter description	Parameter	Description
	network	Default network

Default configuration	0.0.0.0/0
Command mode	Global configuration mode.
Usage guidelines	The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network. The default network always starts with an asterisk (“*”), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.
Examples	The following example sets 192.168.100.0 as the default

network. Since the static route to the network is configured, the device will automatically generate a default route.

```
ip route 192.168.100.0 255.255.255.0 serial 0/1
ip default-network 192.168.100.0
```

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
ip default-network 200.200.200.0
```

Related commands

Command	Description
show ip route	Show the routing table.

1.1.6 ip prefix-list

Use this command to create a prefix list or add an entry to the prefix list. Use the **no** form of this command to remove the prefix list or an entry.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

no ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
seq-number	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry withtout a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
deny	Deny the route matching the prefix list.
permit	Permit the route matching the prefix list.
ip-prefix	Network address nad mask.

	Network address can be any valid IP address and the mask length is in the range of 0 to 32.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
maximum-prefix-length	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and “equivalent to”.

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

The **ip prefix-list** command configures the prefix list, with the **permit** or **deny** keyword to determine the action in case of matching.

You can execute this command to define an exact match, or use “ge” or “ le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 32; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix < minimum-prefix-length < maximum-prefix-length <=32.

Examples

The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24.

```
DES-7200# configure terminal
DES-7200(config)# ip prefix-list pre1 permit 201.1.1.0/24
DES-7200(config)# router ospf
DES-7200(config-router)# distribute-list prefix pre1 out rip
DES-7200(config-router)# end
```

1.1.7 ip prefix-list description

Use this command to add the description of a prefix list. Use the **no** form of this command to delete the description.

ip prefix-list *prefix-list-name* **description** *description-text*

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
description-text	Description of the prefix list

Default configuration

No description is added for a prefix list, by default.

Command mode

Global configuration mode

Examples

The example below adds the description for the prefix list:

```
DES-7200# configure terminal
DES-7200(config)# ip prefix-list pre description Deny routes from Net-A
```

1.1.8 ip prefix-list sequence-number

Use this command to enable sort funciton for a prefix list. Use the **no** form of this command to disable the sort function.

ip prefix-list sequence-number

Parameter description

Disabled

Default configuration

No sequence number is added for a prefix list, by default.

Command mode	Global configuration mode

Examples

The example below adds a sequence number for the prefix list:

```
DES-7200# configure terminal
DES-7200(config)# ip prefix-list pre description deny routes from Net-A
```

Related commands

Command	Description
ip prefix-list	Configure the prefix list.

1.1.9 ip ref ecmp load-balance

Use this command to set the equivalent path selection algorithm of the hardware.

ip ref ecmp load-balance {[crc32_lower | crc32_upper] [dip] [port] [udf *number*]}

no ip ref ecmp load-balance {[crc32_lower | crc32 upper] [dip] [port] [udf *number*]}

Parameter description

Parameter	Description
crc32_upper	Select the high bits of crc32 for the egress nexthhop.
crc32_lower	Select the low bits of crc32 for the egress nexthhop.
dip	Select the destination address as the hash key.
port	Select the tcp/udp port number as the hash key.
udf *number*	Select the user-defined field as the hash key.

Default configuration	crc32_upper.
Command mode	Global configuration mode.

Usage guidelines	This command is used to configure the IPv4/IPV6 ecmp/wcmp path selection algorithm.
Examples	The following example sets the hash algorithm as CRC32_Lower, with the packet keyword being SIP + DIP+TCP/UDP port +UDF: `DES-7200(config)# ip ref ecmp load-balance crc32_lower dip port udf 50`

Related commands

Command	Description
maximum-paths	Configure the number of the equivalent path.

1.1.10 ip route

Use this command to configure a static route. Use the **no** form of this command to remove the configured route.

ip route [**vrf** *vrf_name*] *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent]** [**weight** *number*] [**disable** | **enable**]

no ip route [**vrf** *vrf_name*] *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent]** [**weight** *number*] [**disable** | **enable**]

Parameter description

Parameter	Description
vrf-name	Name of the VRF, which can be the single protocol IPv4 VRF or configured IPv4 address family multi-protocol VRF.
network	Network address of the destination
net-mask	Mask of the destination
ip-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The management distance of the static route
tag	(Optional) The tag of the static route
permanent	(Optional) Permanent rotue ID
number	(Optional) Weight number of the

	static route
disable/enable	(Optional) Disablement or enablement ID of the static route

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

The default management distance of the static route is 1. Setting the management distance allows the learnt dynamic route to overwrite the static route. setting the management distance of the static route can enable route backup, which is called floating route in this case. For example, the management distance of the OSPF is 110. You can set its management distance to 125. Then the data can switch over the static route when the route running OSPF fails.

You can specify the VRF that the static route belongs to.

The default weight of the static route is 1. To view the static route of non default weight, execute the **show ip route weight** command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flows the route carries. WCMP limit is generally 32 for routers. However, WCMP limit varies by switch models for their chipsets support different weights. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it.

When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, ip route 0.0.0.0 0.0.0.0 Fastethernet 0/0. In this case, the switch may consider that all unknown destination networks are directly connected to the Fastethernet 0/0. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not

	recommended to set the static route to an Ethernet interface.

Examples	The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and management distance is 15.
	`ip route 172.16.199.0 255.255.255.0 192.168.12.1 155`
	If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 172.16.100.0/24.
	`ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1`

Related commands	Not supported by layer-2 devices.

1.1.11 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** form of this command to disable the function.

ip routing

no ip routing

Default configuration	Enabled
Command mode	Global configuration mode.
Usage guidelines	IP routing is not necessary when the switch serves as bridge or VoIP gateway.
Examples	The following example disables IP routing `no ip routing`
Related commands	

1.1.12 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** form of this command to restore the setting to the default value.

ip static route-limit *number*

no ip static route-limit *number*

Parameter description

Parameter	Description
number	Upeer threshold of static routes

Default configuration

1024

Command mode

Global configuration mode.

Usage guidelines

The goal is to control the number of static routes. You can view the upeer threshold of the configured non-default static routes with the **show running config** command.

Examples

The following example sets the upeer threshold of the static routes to 900 and then restores the setting to the default value.

```
ip static route-limit 900
```

Related commands

1.1.13 ipv6 prefix-list

Use this command to create an IPv6 prefix list or add an entry in the prefix list. Use the **no** form of this command to delete an IPv6 prefix list or an entry in the prefix list.

Ipv6 prefix-list *prefix-list-name***[seq** *seq-number***] { deny | permit}** *ipv6-prefix* **[ge** *minimum-prefix-length***][le** *maximum-prefix- length***]**

no ipv6 prefix-list *prefix-list-name***[seq** *seq-number***] { deny | permit}** *ipv6-prefix* **[ge** *minimum-prefix- length***][le** *maximum-prefix- length***]**

Parameter description

Parameter	**Description**
prefix-list-name	Name of the prefix list

	seq-number	Sequence number of an entry in the prefix list. Its range is 1 to 4294967294. If the sequence number is not specified in this command, the system will allocate a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one is the product of adding 5 to the sequence number of the proceeding entry.
	permit	Permit the access to the matching result.
	deny	Deny the access to the matching result.
	ipv6-prefix	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
	minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
	maximum-prefix - length	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and “equivalent to”.

Default configuration	No prefix list is created.
Command mode	Global configuration mode
Usage guideline	The **ipv6 prefix-list** command configures the prefix list, with the **permit** or **deny** keyword to determine the action in case of matching. You can execute this command to define an exact match, or use “ge” or “ le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of

	minimum-prefix-length to 128; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, Ipv6-prefix mask length < minimum-prefix-length < maximum-prefix-length <= 128

Examples	The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 2222::/64.
	`DES-7200# configure terminal`
	`DES-7200(config)# ipv6 prefix-list pre1 permit 2222::64`
	`DES-7200(config)# ipv6 router ospf`
	`DES-7200(config-router)# distribute-list prefix pre out rip`
	`DES-7200(config-router)# end`

1.1.14 ipv6 prefix-list description

Use this command to add the description of an IPv6 prefix list. Use the **no** form of this command to delete the description.

ipv6 prefix-list *prefix-lis-name* **description** *description-text*

no ipv6 prefix-list *prefix-lis-name* **description** *description-text*

Parameter description

Parameter	Description
prefix-lis-name	Name of the ipv6 prefix list
description-text	Description of the ipv6 prefix list

Default configuration

No description is added for an IPv6 prefix list, by default.

Command mode

Global configuration mode

Examples	The example below adds the description for the prefix list:
	`DES-7200# configure terminal`
	`DES-7200(config)# ipv6 prefix-list pre description Deny routes from Net-A`

Related commands	Command	Description
	ipv6 prefix-list	Configure the IPv6 prefix list.

1.1.15 ipv6 prefix-list sequence-number

Use this command to enable the sorting function for an IPv6 prefix list. Use the **no** form of this command to remove the settings.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Parameter description	Disabled.
Default configuration	No sequence number is added for a prefix list, by default.
Command mode	Global configuration mode

Examples	The example below adds a sequence number for the prefix list:
	`DES-7200# configure terminal`
	`DES-7200(config)# ipv6 prefix-list pre description Deny routes from Net-A`

Related commands	Command	Description
	ipv6 prefix-list	Configure the IPv6 prefix list.

1.1.16 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** form of this command to delete the configured route.

ipv6 route [vrf *vrf-name***]** *ipv6-prefix/prefix-length* {*ipv6-address* **[nexthop-vrf {***vrf-name1* | **default }]** | *interface* [*ipv6-address*[**nexthop-vrf {***vrf-name1* |**default }]**]} [*distance*] [**weight** *number*]

Parameter description

Parameter	Description
network	Network address of the destination
vrf-name	Name of VRF, which must be the configured IPv6 address family multi-protocol VRF.
prefix-length	Mask length of the destination
Ipv6-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
vrf-name1	VRF the nexthop belongs, which must be the configured IPv6 address family multi-protocol VRF.
distance	(Optional) The management distance of the static route
number	(Optional) The weight value of the static route, which is specified when configuring the equivalent routes,in range of 1 to 128. The sum of the weight of all equivalent paths of one route could not exceed the number of the configurable maximum equivalent paths. The weight ratio between the equivalent routes of the same route shows the flow rate between these paths.

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

When the multi-protocol VRF deletes the IPv6 address family, the IPv6 static route of VRF that the route or nexthop belongs is deleted.

If the VRF of the IPv6 static route interface is not same as the nexthop's VRF, then this IPv6 static route takes no

effect.

The default management distance of the static route is 1. Setting the management distance allows the learnt dynamic route to overwrite the static route. Setting the management distance of the static route can enable route backup, which is called floating route in this case. For example, the management distance of the OSPF is 110. You can set its management distance to 125. Then the data can switch over the static route when the route running OSPF fails.

Examples

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and management distance is 115.

```
ipv6 route 2001::/64 2002::2 115
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 2001::/64.

```
ipv6 route 2001::/64 fastethernet 0/0 2002::2
```

Related commands

Command	Description
show ipv6 route	Show IPv6 routing table .

1.1.17 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** form of this command to restore the setting to the default value.

Ipv6 static route-limit *number*

no ipv6 static route-limit *number*

Parameter description

Parameter	Description
number	Upper threshold of static routes in the range of 1 to 10000.

Default configuration

1000

Command mode	Global configuration mode.
Usage guidelines	The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running config** command.

Examples	The following example sets the upper threshold of the ipv6 static routes to 900 and then restores the setting to the default value.
	`DES-7200# ipv6 static route-limit 900`
	`DES-7200# no ipv6 static route-limit`

Related commands

Command	Description
ipv6 route	Configure the IPv6 static route.
show ipv6 route	Show IPv6 routing table

1.1.18 ipv6 unicast-routing

Use this command to enable the IPv6 route function. Use the **no** form of this command to disable this function.

ipv6 unicast-routing

no ipv6 unicast-routing

Parameter description	None
Default configuration	Enabled
Command mode	Global configuration mode
Usage guidelines	This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

Examples

The example disables the IPv6 route function

```
DES-7200# no ipv6 unicast-routing
```

Related commands

Command	Description
ipv6 route	Configure the IPv6 static route
show ipv6 route	Show the IPv6 routing table

1.1.19 match as-path

Use this command to redistribute the routes of AS_PATH attribute permitted by the access list in the route map configuration mode. Use the **no** form of this command to remove the setting.

match as-path *as-path-acl-list-num* [*as-path-acl-list-num.....*]

no match as-path *as-path-acl-list-num* [*as-path-acl-list-num.....*]

Parameter description

Parameter	Description
as-path-acl-list-num	ACL number, in the range of 1 to 500.
access-list-name	Name of the access list

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

The **match as-path** can be followed by an access list number or name.

One or more **match** or **set** commands can be executed to configure one route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

```
!
route-map ROUTEMAP2IBGP
match as-path 20 30
```

Related commands	Command	Description
	match community	Match the community.
	match metric	Match the metric.
	match origin	Match the source of routes.
	set as-path prepend	Set the AS_PATH attribute of redistributed routes
	set metric	Set the metric.
	set metric-type	Set the metric type.

1.1.20 match community

Use this command to redistribute the routes matching the Community attribute permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match community { *community-list-number* | *community-list-name*} [**exact-match**] [{*community-list-number* | *community-list-name*} [**exact-match**] …]

no match community { *community-list-number* | *community-list-name*} [**exact-match**] [{ *community-list-number* | *community-list-name*} [**exact-match**] …]

Parameter description	Parameter	Description
	community-list-number	Number of the standard community list in the range 1 to 99. Number of the extended community list in the range of 100 to 199
	communitys-list-name	Name of the community list in the range of less than 80 characters
	exact-match	Match the community list exactly.

Default configuration	None.

Command mode	Route map configuration mode.

Usage guidelines

The **match community** can be followed by more than one community list number or name, but the total of community lists and names should not be greater than 6.

Each exact-match applies to only the previous list, not all the lists.

One or more **match** or **set** commands can be executed to configure one route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

```
ip community-list 1 permit 100:2 100:30
route-map set lopref
match community 1 exact-match
set local-preference 20
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

1.1.21 match interface

Use **match interface** command to redistribute the routes whose next hop is the specified interface. Use the **no** form of this command to remove the setting.

match interface *interface-type interface-number* [*…interface-type interface-number*]

no match interface *[interface-type interface-number* [*…interface-type interface-number*]]

Parameter description

Parameter	Description
interface-type	Interface type
interface-number	Interface number

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

This command can be followed by multiple interfaces.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match interface fastethernet 0/0
```

Related commands

Command	Description
match ip address	Match the address in the access list.
match ip next-hop	Match the next-hop IP address in the access list.
match ip route-source	Match the source IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.

match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.22 match ip address

Use **match ip address** command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the **no** form of this command to remove the setting.

match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip address [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow **match ip address**.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type-1 external type and the default metric being 40.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 200.168.23.0

route-map redrip permit 10
match ip address 10
set metric 40
set metric-type type-1!
```

Related commands

Command	Description
access-list	Set the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop address in the access list.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.23 match ip next-hop

Use **match ip next-hop** command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the **no** form of this command to remove the setting.

match ip next-hop {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip next-hop [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow **match ip next-hop**.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 192.168.100.1
access-list 20 permit 172.16.10.1

route-map redrip permit 10
match ip next-hop 10 20
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.24 match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list. Use the **no** form of this command to remove the setting.

match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip route-source [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers may follow **match ip route-source**.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the source IP address of the RIP route matches the access list 5, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 5 permit 192.168.100.1

route-map redrip permit 10
 match ip route-source
```

Related commands	

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.25 match ipv6 address

Use this command to redistribute the network routes permitted in the IPv6 access list or the IPv6 prfix list. Use the **no** form of this command to delete the setting.

match ipv6 address { *access-list-name*] | **prefix-list** *prefix-list-name* }

no match ipv6 address

Parameter description

Parameter	Description
access-list-name	Name of the access list.
prefix-list prefix-list-name	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage

You can redistribute the routing information from one routing process to another routing process. For example,

guideline

you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list v6acl, with the default metric being 30.

```
ipv6 router ospf
redistribute rip subnets route-map redrip
ipv6 access-list v6acl
10 permit ipv6 2620::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 30
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 next-hop	Match the next-hop address in the IPv6 access list.
match ipvr route-source	Match the route source address in the IPv6 access list.

match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

1.1.26 match ipv6 next-hop

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 next-hop { *access-list-name*] | **prefix-list** *prefix-list-name*}

no match ipv6 next hop

Parameter description

Parameter	Description
access-list-name	Name of the IPv6 access list.
prefix-list prefix-list-name	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 40.

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 2620::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 40
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.

match ipv6 route-source	Match the route source address in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

1.1.27 match ipv6 route-source

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 route-source { *access-list-name*] | **prefix-list** *prefix-list-name* }

no match ipv6 route-source

Parameter description

Parameter	Description
access-list-name	Name of the IPv6 access list.
prefix-list prefix-list-name	Specify the IPv6 prefix list to match.

Default configuration None

Command mode Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 50.

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 5200::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 50
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.

match ipv6 next-hop	Match the next hop in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

1.1.28 match metric

Use **match metric** command to redistribute the routes of the specified metric. Use the **no** form of this command to remove the setting.

match metric *metric*

no match metric *metric*

Parameter description

Parameter	Description
metric	Route metric, in the range 0 to 4294967295

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set

commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10.

```
router ospf 1
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match metric 10
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.29 match origin

Use this command to redistribute the routes whose source IP address is permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match origin {egp | igp | incomplete}

no match origin [egp | igp | incomplete]

Parameter description

Parameter	Description
egp	Redistribute the routes from the remote EGP.

igp	Redistribute the routes from the local IGP.
incomplete	Redistribute the routes from an imcomplete type.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the origin of the routes to be redistributed. Only one origin can be set.

Examples

```
DES-7200(config)# route-map MY_MAP 10 permit
DES-7200(config-route-map)# match origin egp
DES-7200(config-route-map)# set community 109
DES-7200(config-route-map)# exit
DES-7200(config)# route-map MAP20 20 permit
DES-7200(config-route-map)# match origin incomplete
DES-7200(config-route-map)# set community no-export
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set origin	Set the source.

1.1.30 match route-type

Use this command to redistribute the network routes of the specified type. Use the **no** form of this command to delete the setting.

match route-type {**local | internal** | **external** [**type-1** | **type-2**] | **level-1 | level-2 | sdg_owner | sdg_slave**}

no match route-type [**local | internal** | **external** [**type-1** | **type-2**] | **level-1 | level-2 | sdg_owner | sdg_slave**]

Parameter description

Parameter	Description
local	Resdistribute the local rotues.
internal	Redistribute the routes in the OSPF routing domain.
external	Redistribute the routes out of the BGP or OSPF routing domain.
type-1 | type-2	Redistribute the OSPF type-1 or type-2 routes.
level-1 | level-2	Redistribute the ISIS level-1 or level-2 routes.
sdg_owner	SDG master route.
sdg_slaver	SDG slaver route.

Default configuration None

Command mode Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain.

```
router rip
redistribute ospf route-map redrip
network 192.168.12.0

route-map redrip permit 10
match route-type internal
!
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the access list.
set tag	Match the IP address.

1.1.31 match tag

Use this command to redistribute the network routes with the specified tag. Use the **no** form of this command to delete the setting.

match tag *tag* [*…tag*]

no match tag [*tag* [*…tag*]]

Parameter description

Parameter	Description
tag	Route tag

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Multiple tags may follow the **match tag** command.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain.

```
router rip
redistribute ospf 100 route-map redrip
network 192.168.12.0

route-map redrip permit 10
match tag 50 80
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the next-hop IP interface.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match ip next-hop	Match the next-hop IP address.
match route-type	Match the route type.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.32 maximum-paths

Use this command to specify the number of equivalent routes. The **no** form of this command is used to restore the setting to the default value.

maximum-paths *number*

no maximum-paths *number*

Parameter description

Parameter	Description
number	Number of equivalent routes in the range of 1 to 32

Default configuration

32 for routers. For switches, it depends on switch models.

Command mode	Route map configuration mode.
Usage guidelines	With this command executed, the number of routes for load balancing is no more than the specified number of equivalent routes. You can view the number of equivalent routes with the **show running config** command.

Examples	The following example sets the number of equivalent routes to 10 and then restore it to the default value.
	`maximum-paths 10`
	`no maximum-paths 10`

1.1.33 route-map

Use **route-map** to enter the route map configuration mode and define a route map. Use the **no** form of this command to remove the setting.

route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

no route-map *route-map-name* [{**permit** | **deny**}*sequence-number*]

Parameter description

Parameter	Description
route-map-name	Name of the route map. The **redistribute** command references the route map according to its name. Multiple routing policies can be defined in a route map, and each policy corresponds to one sequence number.
permit	(Optional) If the **permit** keyword is defined and the rule defined by **match** is met, The **set** command controls the redistributed routes. For policy-based routing, the **set** command controls the packet forwarding, and exits the route map operation. If the **permit** keyword is defined but the rule defined by **match** is not met, the system performs the routing policy of the second route map till the **set** command is executed finally.

	deny	(Optional) If the **deny** keyword is defined and the rule defined by **match** is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation. If the **deny** keyword is defined but the rule defined by **match** is not met, the system performs the routing policy of the second route map till the **set** command is executed finally.
	sequence-number	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

Default configuration

None.

Command mode

Global configuration mode.

Usage guidelines

At present, the route map is used for route redistribution and policy-based routing.

1. Route redistribution control

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

1) When you create the first route map policy, if *sequence-number* is not specified, it is 10 by default;
2) If only one route map policy exists and *sequence-number* is not specified, no new route map policy will be created, and the existing route map policy will be accessed for configuration;

If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed.

2. policy-based routing

Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The **match** command defines packet filtering rule and the **set** command defines the action for the packets matching the filtering rules. The **match** command used includes **match ip address**; the **set** command includes **set ip tos**, **set ip precedence**, **set ip dscp**, **set ip [default] nexthop**, **set ip next-hop verify-availability**.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the hop count of 4. In the OSPF route domain, the route type is the external route type-1, the default metric is 40 and the tag is 40.

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
!
route-map redrip permit 10
 match metric 4
 set metric 40
 set metric-type type-1
 set tag 40
```

Related commands

Command	Description
redistribute	Redistribute the routes.

1.1.34 set aggregator as

Use this command to specify the AS_PATH attribute for the aggregator of the routes that match the rule in the route map configuration mode. Excute the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set aggregator as *as-number ip_addr*

no set aggregator as [*as-number ip_addr*]

Parameter description

Parameter	Description
as-number	AS number of the aggregator
ip_address	IP address of the aggregator

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the AS_PATH attribute for the matched routes in the BGP routing domain. Only one group of parameters (as-number, ip-addr) is allowed to set at a time.

Examples

```
DES-7200(config)# route-map set-as-path
DES-7200(config-route-map)# match as-path 1
DES-7200(config-route-map)# set aggregator as 3 2.2.2.2
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the route metric.

match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

1.1.35 set as-path prepend

Use this command to specify the AS_PATH attribute for the routes that match the rule in the route map configuration mode. Excute the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set as-path prepend *as-number*

no set as-path prepend

Parameter description

Parameter	Description
as-number	AS number of the AS_PATH attribute to be configured. The AS number ranges from 1 to 4294967295, and 1 to 65535.65535 in dot mode.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to configure the AS_PATH attribute for the matched routes. Up to 15 ass can be added into the as-path for one time.

Examples

```
DES-7200(config)# route-map set-as-path
DES-7200(config-route-map)# match as-path 1
DES-7200(config-route-map)# set as-path prepend 100 101 102
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the route metric.
match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

1.1.36 set comm-list delete

Use this command to delete the COMMUNITY_LIST attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set comm-list *community-list-number* | *community-list-name* **delete**

no set comm-list *community-list-number* | *community-list-name* **delete**

Parameter description

Parameter	Description
community-list-number	Number of the community list. Standard community list number : 1-99. extended community list number : 100-199.
community-list-name	Name of the community list, which should be no more than 80 characters.

Default configuration None

Command mode Route map configuration mode

Usage guideline

Use this command to set the community attribute value for the matched routes that will be deleted.

Examples

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# neighbor 172.16.233.33 remote-as 120
DES-7200(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPIN in
DES-7200(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out
DES-7200(config-router)# exit
DES-7200(config)# ip community-list 500 permit 100:10
DES-7200(config)# ip community-list 500 permit 100:20
DES-7200(config)# ip community-list 120 deny 100:50
DES-7200(config)# ip community-list 120 permit 100:.*
DES-7200(config)# route-map ROUTEMAPIN permit 10
DES-7200(config-route-map)# set comm-list 500 delete
DES-7200(config-route-map)# exit
DES-7200(config)# route-map ROUTEMAPOUT permit 10
DES-7200(config-route-map)# set comm-list 120 delete
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute value.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set local-preference	Set the local priority of the route to be redistributed.
set metric-type	Set the metric type.

1.1.37 set community

Use this command to specify the community for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set community {*community-number*[community-number…] [**additive | none**}

no set community

Parameter description

Parameter	Description
community-number	Community number in the form of AA:NN or a large numeral. In addition, it can be well-known community attributes like **internet**, **local-AS**, **no-export** and **no-advertise**.
additive	Increase on the original COMMUNITY attribute.
none	Set the community attribute as blank.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the community attribute for the matched route.

Examples

```
DES-7200(config)# route-map SET_COMMUNITY 10 permit
DES-7200(config-route-map)# match as-path 1
DES-7200(config-route-map)# set community 109:10
DES-7200(config-route-map)# exit
DES-7200(config)# route-map SET_COMMUNITY 20 permit
DES-7200(config-route-map)# match as-path 2
DES-7200(config-route-map)# set community no-export
```

Related commands

Command	Description
match as-path	Match the AS_PATH.

match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set origin	Set the source.
set metric-type	Set the metric type.

1.1.38 set dampening

Use this command to specify the dampening parameters for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Parameter description

Parameter	Description
half-life	Half dampening life for the reachable or unreachable route in the range of 1 to 45 minutes, 15 minutes by default
reuse	When the route penalty is lower than this value, the route suppression is released. It is in the range 1 to 20000, 750 by default
suppress	When the route penalty is higher than this value, the route is suppressed. It is in the range 1 to 20000, 2000 by default
max-suppress-time	Maximum duration a route can be suppressed in the range 1 to 20000 minutes, 4* half-life by default.

Default configuration None

Command mode	Route map configuration mode
Usage guideline	Use this command to set the dampening parameter for the matched routes.

Examples	`DES-7200(config)# route-map tag`
	`DES-7200(config-route-map)# match as path 10`
	`DES-7200(config-route-map)# set dampening 30 1500 10000 120`
	`DES-7200(config-route-map)# exit`
	`DES-7200(config)# router bgp 100`
	`DES-7200(config-router)# neighbor 172.16.233.52 route-map tag in`

Related commands

Command	Description
match as-path	Match the AS_PATH value.
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of the route to be redistributed.

1.1.39 set extcommunity

Use this command to specify the extended COMMUNITY attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set extcommunity {**rt** *extend-community-value* | **soo** *extend-community-value*}

no set extcommunity {**rt** | **soo** }

Parameter description

Parameter	Description
rt	Specify the extended community value in the form of RT.
soo	Specify the extended community value in the form of SOO.
extend-community-value	Extended community value.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the extended community attribute for the matched route.

Examples

```
DES-7200(config)# access-list 2 permit 192.168.78.0 255.255.255.0
DES-7200(config)# route-map MAP_NAME permit 10
DES-7200(config-route-map)# match ip-address 2
DES-7200(config-route-map)# set extcommunity rt 100:2
```

Related commands

Command	Description
match as-path	Match the AS_PATH value
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

1.1.40 set ip default next-hop

Use this command to specify the default next-hop IP address for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip default next-hop *ip-address* [*weight*] […*ip-address*[*weight*]]

no set ip default next-hop [*ip-address* [weight] […*ip-address*[*weight*]]]

Parameter description

Parameter	Description
ip-address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline	This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight inputted. Up to 32 IP addresses may follow the set ip default next-hop command. If a weight follows ip address, up to 4 next hop IP addresses can be configured. Note: If a weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In this mode, the weight of those next hop IP addresses whose weight is not configured is 1 by default. Differences between set ip next-hop and set ip default next-hop: After the set ip next-hop command is configured, the policy-based routing takes precedence over the routing table; while after the set ip default next-hop command is configured, the routing table takes precedence over the policy-based routing. Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packet will be forwarded to the nexthop set with this command. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded through the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. A route-map policy may contain multiple **set** operations.
Examples	The following example forwards the packets from two different nodes through different routes. For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to device 6.6.6.6. For the messages received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to device 7.7.7.7.

```
DES-7200(config)#access-list 1 permit 1.1.1.1 0.0.0.0
DES-7200(config)#access-list 2 permit 2.2.2.2 0.0.0.0
DES-7200(config)#interface async 1
DES-7200(config-if)#ip policy route-map equal-access
DES-7200(config)#route-map equal-access permit 10
DES-7200(config- route-map)#match ip address 1
DES-7200(config-route-map)#set ip default next-hop 6.6.6.6
DES-7200(config)#route-map equal-access permit 20
DES-7200(config-route-map)#match ip address 2
DES-7200(config-route-map)#set ip default next-hop 7.7.7.7
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

1.1.41 set ip dscp

Use this command to specify the DSCP value for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip dscp *dscp-value*

no set ip dscp

Parameter description

Parameter	Description
dscp-value	DSCP value

Default configuration N/A

Command mode	Route map configuration mode
Usage guideline	N/A
Examples	N/A

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

1.1.42 set ip next-hop

Use this command to specify the next-hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop *ip-address* [weight] […*ip-address* [*weight*]]

no set ip next-hop [*ip-address* [weight] […*ip-address*[*weight*]]]

Parameter description

Parameter	Description
ip-address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration	None
Command mode	Route map configuration mode

This command supports two operation modes: **WCMP** load balancing mode and **non-WCMP** load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow **set ip next-hop** and the number of addresses should be less than 32.

If **weight** follows **ip address**, up to 4 next hop addresses can be configured.

Caution

If **weight** follows any **next-hop**, the operation mode of this command will be automatically switched to the **WCMP** load balancing mode. In the WCMP load balancing mode, for the **nexthop address** without configuring the corresponding **weight**, the **weight** is 1 by default.

Usage guideline

This command can be used to set different routes for the traffic that meets different **match** rule. If multiple IP addresses are configured, they can be used in turn.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. After the policy-based routing is used, the device will decide how to process the packets that need be routed according to the route map, which decides the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple **set** operations.

Examples

The following example enables policy-based routing on serial 1/0. When the interface receives the packets from

10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets from 172.16.0.0/16, they will be sent to 172.16.100.1.

```
DES-7200(config)#interface serial 1/0
DES-7200(config-if)#ip policy route-map load-balance
DES-7200(config)#access-list 10 permit 10.0.0.0 0.255.255.255
DES-7200(config)#access-list 20 permit 172.16.0.0 0.0.255.255
DES-7200(config)#route-map load-balance permit 10
DES-7200(config-route-map)#match ip address 10
DES-7200(config-route-map)#set ip next-hop 192.168.100.1
DES-7200(config)#route-map load-balance permit 20
DES-7200(config-route-map)#match ip address 20
DES-7200(config-route-map)#set ip next-hop 172.16.100.1
```

Related commands

Command	Description
Route-map	Define the route map.
match ip address	Match the IP address.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

1.1.43 set ip next-hop verify-availability

Use this command to verify the availability of the next hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop verify-availability *ip-address* **track** *track-object-num*

no set ip next-hop verify-availability

Parameter description

Parameter	Description
ip-address	IP address of the next hop
track-object-num	Number of the object to be tracked

Default configuration	None
Command mode	Route map configuration mode
Usage guideline	None

Examples	The following example verifies the availability of the next hop IP address being 192.168.1.2 and the number of the object to be tracked to 1.
	`DES-7200(config)#route-map rmap permit 10`
	`DES-7200(config-route-map)#set ip next-hop verify-availability 192.168.1.2 track 1`

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

1.1.44 set ip precedence

Use this command to set the precedence of the IP head of the packet matching the rule in the route map configuratio mode. Use the **no** form of this command to remove the configured precedence setting.

set ip precedence {*<0-7>* | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ip precedence

Default configuration	N/A

Command mode

Route map configuration mode

Usage guideline

With different precedence values for the IP packet head configured, the IP packets matching the PBR routing are sent accoding to the different precedence values.

Multiple **set ip precedence** commands can be executed in the route map configuration rule, but only the last one takes effect, and the precedence will be specified for the head of the IP packet matiched the PBR.

Examples

The following example sets the precedence of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

```
DES-7200(config)#access-list 1 permit 192.168.217.68 0.0.0.0

DES-7200(config)#route-map name

DES-7200(config-route-map)#match ip address 1

DES-7200(config-route-map)#set ip precedence 4

DES-7200(config)#interface FastEthernet 0/0

DES-7200(config-if)#ip policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.

set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip tos	Set the tos for the IP packet head.

1.1.45 set ip tos

Use this command to set the tos of the IP head of the packet matching the rule in the route map configuratio mode. Use the **no** form of this command to remove the configured tos setting.

set ip tos {*<0-15>* | *max-reliability* | *max-throughput* | *min-delay* | *min-monetary-cost* | *normal* }

no set ip tos

Default configuration	N/A
Command mode	Route map configuration mode
Usage guideline	With different TOS values for the IP packet head configured, the IP packets matching the PBR routing are transmitted with different service qualities. The TOS value will be specified for the head of the IP packet matched the PBR.

Examples	The following example sets the TOS value of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:
	`DES-7200(config)#access-list 1 permit 192.168.217.68 0.0.0.0`
	`DES-7200(config)#route-map name`
	`DES-7200(config-route-map)#match ip address 1`

```
DES-7200(config-route-map)#set ip tos 4

DES-7200(config)#interface FastEthernet 0/0

DES-7200(config-if)#ip policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip precedence	Set the precedence for the IP packet head.

1.1.46 set ipv6 default next-hop

Use this command to specify the default next-hop IPv6 address for the IPv6 packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ipv6 default next-hop *global-ipv6-address* [*weight*] […*ipv6-address*[*weight*]]

no set ipv6 default next-hop *glocal-ipv6-address* [weight] […*ipv6-address*[*weight*]]

Parameter description

Parameter	Description
global-ipv6-address	IPv6 address of the next hop. The next hop router must be the neighbor router.

weight	Weight in the load balancing mode, in the range of 1 to 8.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

With the policy-based routing applied to the interface, for the IPv6 packets matching the corresponding rules, if the usual route (that is the non default route) with the destination of this packet is not in the routing table, this packet will be forwarded to the next hop specified by the **set ipv6 default next-hop** command. Otherwise it is forwarded through the usual route. Noted that the match rule should be the IPv6 corresponded.

Packets select the egress from the policy-based routing and routing table in following priority.

- set ipv6 next-hop;
- usual route (the non default route)
- set ipv6 default next-hop
- default route.

Caution

For the switches, this function does not take effect if the mask length is beyond 64.

If this command and the **set ipv6 next-hop verify-availability** are both configured ,the next hop set by the **set ipv6 next-hop verify-availability** command will take effect preferentially

Examples

The following examle sets the default next hop of the packet with destination address *2001:0db8:2001:1760::/64* received at the interface fastEthernet 0/0 as *2002:0db8:2003:1::95*

```
DES-7200(config)# ipv6 access-list acl_for_pbr

DES-7200(config-ipv6-acl)#permit        ipv6        any
```

```
2001:0db8:2001:1760::/64

DES-7200(config)#route-map rm_if_0_0

DES-7200(config-route-map)#match ipv6 address
acl_for_pbr

DES-7200(config-route-map)# set ipv6 default next-hop

2002:0db8:2003:1::95

DES-7200(config)#interface FastEthernet 0/0

DES-7200(config-if)#ipv6 policy route-map rm_if_0_0
```

Related commands

Command	Description
match ipv6 address	Set the matching rule of policy-based routing.
ipv6 policy route-map	Use the policy-based routing on the interface.
set ipv6 next-hop	Set the next hop of the policy-based routing.

1.1.47 set ipv6 next-hop

Use this command to specify the next-hop IPv6 address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ipv6 next-hop [vrf *vrf-name* **| global]** *global-ipv6-address* [weight] [*…global-ipv6-address* [*weight*]]

no set ip next-hop [vrf *vrf-name* **| global]** *global-ipv6-address* [weight] [*…global-ipv6-address* [*weight*]]

Parameter description

Parameter	Description
global-ipv6-address	IPv6 address of the next hop. The next hop router should be the neighbor router.
vrf *vrf-name*	The nexthop belongs to the specified VRF which must be the configured IPv6 address family multi-protocol VRF.
global	The nexthop belongs to the global.

weight	Weight of the next hop in the load balancing mode, in the range of 1to 8.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

This command supports two operation modes: **WCMP** load balancing mode and **non-WCMP** load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow **set ip next-hop** and the number of addresses should be less than 32.

If **weight** follows **ip address**, up to 4 next hop addresses can be configured.

If the parameter **vrf** *vrf-name* is specified, packets forwarding will be across the VRF. The packets wil be forwarded from VRF to pubic network with the parameter **global** specified. If no **[vrf** *vrf-name* **| global]** is specified, forwarding the IPv6 packets will inherit the VRF, that is the nexthop belongs to the VRF that receives this IPv6 packets.

Caution

If **weight** follows any **next-hop**, the operation mode of this command will be automatically switched to the **WCMP** load balancing mode. In the WCMP load balancing mode, for the **nexthop address** without configuring the corresponding **weight**, the **weight** is 1 by default.

When the packets select the egress from the policy-based routing and routing table, the priorities are as bellows.

- set ipv6 next-hop；
- usual route (the non default route)
- set ipv6 default next-hop

■ Default route.

Examples

The following examle sets the next hop of the packet with destination address *2001:0db8:2001:1760::/64* received at the interface fastEthernet 0/0 as *2002:0db8:2003:1::95*

```
DES-7200(config)# ipv6 access-list acl_for_pbr
DES-7200(config-ipv6-acl)#permit ipv6 any 2001:0db8:2001:1760::/64
DES-7200(config)#route-map rm_if_0_0
DES-7200(config-route-map)#match ipv6 address acl_for_pbr
DES-7200(config-route-map)# set ipv6 next-hop 2002:0db8:2003:1::95
DES-7200(config)#interface FastEthernet 0/0
DES-7200(config-if)#ipv6 policy route-map rm_if_0_0
```

Related commands

Command	Description
match ipv6 address	Set the matching rule of policy-based routing.
ipv6 policy route-map	Use the policy-based routing on the interface.
set ipv6 next-hop	Set the next hop of the policy-based routing.

1.1.48 set ipv6 precedence

Use this command to set the precedence of the IPv6 head of the packet matching the rule in the route map configuratio mode. Use the **no** form of this command to remove the configured precedence setting.

set ipv6 precedence {*<0-7>* | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ipv6 precedence {*<0-7>* | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

Parameter description

Parameter	Description
critical、flash、flash-override、immediate、internet、network、priority、routine	The precedence type of the IPv6 head.
0~7	The configurable precedence range.

Default configuration

N/A

Command mode

Route map configuration mode

Usage guideline

The following table shows the corresponding relationship between the value and type.

Value	Type
0	routing
1	priority
2	network
3	internet
4	immediate
5	flash-override
6	flash
7	critical

Examples

The following example sets the precedence of IPv6 packet head as 3:

- Configure the associated ACL6

```
DES-7200(config)#ipv6 access-list aaa

DES-7200(config-ipv6-acl)#permit ipv6 2003:1000::10/80
2001:100::/64
```

- Configure route-map.

```
DES-7200(config)#route-map pbr-aaa permit 10
DES-7200(config-route-map)#set ipv6 next-hop 2001:1234::2
```

- Modify the precedence.

```
DES-7200(config-route-map)# set ipv6 precedence 3
Or
DES-7200(config-route-map)# set ipv6 precedence immediate
```

Related commands

Command	Description
match ipv6 address	Configure the ACL used for matching the packet in IPv6 PBR.
route-map	Use the route map of the policy-based routing.
set ipv6 default next-hop	Set the default next-hop address for forwarding packets.
set ipv6 next-hop	Set the next-hop address for forwarding packet.
show ipv6 policy	Show the policy-based routing
show route-map	Show the route map configuraiton.

1.1.49 set level

Use this command to set the level of the area where the routes matching the rule are redistributed in the route map configuration command. Use the **no** form of this command to remove the setting.

set level {level-1| level-2 | level-1-2 | stub-area | backbone}

no set level

Default configuration None

Command mode	Route map configuration mode

Examples

In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area.

```
DES-7200(config)# router ospf
DES-7200(config-router)# redistribute rip subnets route-map redrip
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7200(config-router)# exit
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# set level backbone
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.50 set local-preference

Use this command to set the **LOCAL_PREFERENCE** value for the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting. **set local-preference** *number*

no set local-preference

Parameter description

Parameter	Description
number	Local priority metric ranging 1 to 4294967295

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the local preference for the matched routes. Only one local preference can be set.

Examples

```
DES-7200(config)# route-map SET_PREF permit 10
DES-7200(config-route-map)# match as-path 1
DES-7200(config-route-map)# set local-preference 6800
DES-7200(config-route-map)# exit
DES-7200(config)# route-map SET_PREF permit 20
DES-7200(config-route-map)# match as-path 2
DES-7200(config-route-map)# set local-preference 50
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

1.1.51 set metric

Use **set metric** to set the metric for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric [+ *metric-value* | **-** *metric-value* | *metric-value*]

no set metric

Parameter description

Parameter	Description
+	Increase based on the metric of the original route
-	Decrease based on the metric of the original route
metric-value	Metric for the route to be redistributed

Default configuration

The default metric for route redistribution varies with the routing protocol.

Command mode

Route map configuration mode

Usage guideline

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attentions should be paid to the upeer and lower limits of the routing protocols when you execute the **set metric**, **+ metric** or **– metric** commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes and sets the default metric to 40.

```
DES-7200(config)# router ospf
DES-7200(config-router)# redistribute rip subnets route-map redrip
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7200(config-router)# exit
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# set metric 40
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.

match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.52 set metric-type

Use **set metric-type** to set the type of the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric-type *type*

no set metric-type

Parameter description

Parameter	Description
type	Type of the routes to be redistributed. At present, you can set the type of the routes that the OSPF protocol redistributes. type-1: Type-1 external route; type-2: Type-2 external route.

Default configuration

Type-2

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing

domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.

```
DES-7200(config)# router ospf
DES-7200(config-router)# redistribute rip subnets route-map redrip
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7200(config-router)# exit
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# set metric-type type-1
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set tag	Set the tag.

1.1.53 set next-hop

Use this command to specify the next-hop IP address for the routes that match the rule. Use the **no** form of this command to remove the setting. This command is only used to configure routing policies.

set next-hop *ip-address*

no set next-hop

Parameter description

Parameter	Description
ip-address	IP address of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2.

```
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# match ip address 1
DES-7200(config-route-map)# set next-hop 192.168.1.2
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.

match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

1.1.54 set origin

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set origin {egp | igp | incomplete}

no set origin {egp | igp | incomplete}

Parameter description

Parameter	Description
egp	Redistribute the routes from the remote EGP.
igp	Redistribute the routes from the local IGP.
Incomplete	Redistribute the routes from an unknown device.

Default configuration None

Command mode Route map configuration mode

Usage guideline Use this command to set the source of the routes to be matched. Only one route source attribute can be set.

Examples

```
DES-7200(config)# route-map SET_ORIGIN 10 permit
DES-7200(config-route-map)# match as-path 1
DES-7200(config-route-map)# set origin igp
DES-7200(config-route-map)# exit
DES-7200(config)# route-map SET_ORIGIN 20 permit
DES-7200(config-route-map)# match as-path 2
DES-7200(config-route-map)# set origin egp
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of redistributed routes.

1.1.55 set originator-id

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set originator-id *ip-addr*

no set originator-id [*ip-addr*]

Parameter description

Parameter	Description
ip-addr	IP address of the originator.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the source of the routes to be matched.

Examples

```
DES-7200(config)# route-map SET_ORIGIN 10 permit
DES-7200(config-route-map)# match as-path 1
DES-7200(config-route-map)# set originator-id 5.5.5.5
DES-7200(config-route-map)# exit
DES-7200(config)# route-map SET_ORIGIN 20 permit
DES-7200(config-route-map)# match as-path 2
DES-7200(config-route-map)# set originator-id 5.5.5.6
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of redistributed routes.

1.1.56 set vrf

Use this command to forward the IP packets that match the rule according to the specified VRF routing table. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set vrf *name*

no set vrf *name*

Parameter description

Parameter	Description
name	Name of the VRF instance

Default configuration	None

Command mode	Route map configuration mode

Usage guideline

When specify the multi-protocol VRF without the IPv4 address family configured, the IPv4 PBR takes no effect. With no IPv6 address family configured, the IPv6 PBR is not effective. With the IPv4 and IPv6 address families configured, the set vrf rule is valid for the IPv4 PBR and IPv6 PBR.

Use this command to forward the IP packet that match different rule according to different VRF table.

If the uni-protocol IPv4 VRF is specified, the IPv6 PBR is not effective.

1，Before configuring the **set vrf** command, the VRF must exist. If the specified VRF does not exist, it will prompt the fault message. The setting that uses the VRF instance will be removed after removing this VRF instance.

a) If the VRF specified by this command does not exist, it will prompt: %route-map：VRF table vrf-name does not exist.

b) When removing the VRF, the corresponding set vrf configuration is removed synchronously, it will prompt: %route-map:set vrf vrf-name configuration removed from all route-maps.

2. In the same policy of the route map, the commands: **set vrf ,set ip nexthop, set ip next-hop verify-availability** could not be configured altogether，but the command **set vrf ,set ip tos,set ip precedence,set ip dhcp** can be configured altogether. If the **set vrf** command is executed many times in the same policy of the route map, the latter configuration will overwrite the former s without any prompt message.

In the same policy of the route map, if the **set ip nexthop** command is set before the **set vrf** ,it will prompt :

% route-map：can not set vrf .

% Remove other set clauses to set vrf.

From the version 10.4(3), the **set vrf, set ip nexthop** and **set ipv6 next-hop** commands can be configured in the same policy of the route map at the same time. The **set vrf** has the higher priority than the **set ip nexthop** and **set ipv6 next-hop**.

Examples

In the examples below, the policy-based routing is enabled on serial 1/0 to forward the traffic whose destination

address is in the range of 10.0.0.0/8 through the vrf_A table, and the traffic whose destination address is in the range of 172.16.0.0/16 through the vrf_B table, and the remaining traffic through the global routing table.

The example1 defines the ACL

```
DES-7200(config)# access-list 10 permit 10.0.0.0 0.255.255.255
DES-7200(config)# access-list 20 permit 172.16.0.0 0.0.255.255
```

The example2 configures the route-map

```
DES-7200(config)#route-map PBR permit 10
DES-7200(config-route-map)#match ip address 10
DES-7200(config-route-map)#set vrf vrf_A
DES-7200(config)#route-map PBR permit 20
DES-7200(config-route-map)#match ip address 20
DES-7200(config-route-map)#set vrf vrf_B
```

The example3 configures the policy-based routing on the interface.

```
DES-7200(config)#interface serial 1/0
DES-7200(config-if)#ip policy route-map PBR
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
ip vrf receive	Add the direct-conneting route and the host route of one interface to the specified VRF routing table.
vrf receive	Import an IPv6/v6 local host route and direct route of a interface to the VRF routing table specified by the vrf_name.

1.1.57 set tag

Use this command to set the tag for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set tag *tag*

no set tag

Parameter description

Parameter	Description
tag	Tag of the route to be redistributed

Default configuration

The original routing tag remains unchanged.

Command mode

Route map configuration mode

Usage guideline

This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.

```
DES-7200(config)# router ospf
DES-7200(config-router)# redistribute rip subnets route-map redrip
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7200(config-router)# exit
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# set tag 100
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.

match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.

1.1.58 set weight

Use this command to set the weight for the BGP routes matching filtering rules. Use the **no** form of this command to remove the setting.

set weight *number*

no set weight

Parameter description

Parameter	Description
number	Weight in the range of 0 to 65535

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

This command can only be used modify the weight of a BGP route.

By default, the weight of the route learned from a neighbor is the one configured with the **neighbor weight** command. The weight of the locally generated route is fixed 32768.

Examples

The following example sets the weight for the BGP route learned from the neighbor 1.1.1.1 at the inbound direction to 100.

```
DES-7200(config)# router bgp 1
```

```
DES-7200(config-router)# neighbor 1.1.1.1 route-map nei-rmap-in in
DES-7200(config-router)# exit
DES-7200(config)# route-map nei-rmap-in permit 10
DES-7200(config-route-map)# set weight 100
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match community	Match the route community.
match metric	Match the route metric.
match origin	Match the source.
set community	Set community of the redistributed route.
set metric	Set the metric of the redistributed route.
set metric type	Set the metric type of the redistributed route.

1.2 Show Related Command

1.2.1 show dampening interface

Use this command to show the statistical information of the danmpening interface.

show dampening interface

Parameter description

Parameter	Description
-	-

Default N/A

Command mode Privileged mode.

Usage guidelines	N/A

Examples	The following example shows the statistical information of the dampening interface.
	`DES-7200# show dampening interface`
	`3 interfaces are configured with dampening.`
	`No interface is being suppressed.`

Related commands

Command	Description
dampening	Enable the ip event dampening function on the interface.
clear counters	Clear the interface counters.
show interface dampening	Show the detailed information of the ip event dampening function on all interfaces.

1.2.2 show interface dampening

Use this command to show the detailed dampening information on all interfaces.

show interface [*interface-id***] dampening**

Parameter description

Parameter	Description
interface-id	Interface name, such as gigabitEthernet 0/1.

Default	N/A
Command mode	Privileged mode.
Usage guidelines	If the interface-id is specified, only the dampening information of this specified interface is shown.
Examples	The following example shows the detailed dampening

information on all interfaces.

```
DES-7200# show interface dampening Ethernet1/0
Flaps  Penalty  Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP
Restart
  0     0     FALSE   0     5    1000  2000   20    16000
  0
```

Domain	Description
Flaps	Interface flapping times.
Penalty	The current penalty value on the interface.
Supp	Suppressed or not.
ReuseTm	Time to unsuppress the interface, in seconds.
HalfL	Half-life period, in seconds.
ReuseV	Unsuppressed threshold.
SuppV	Start suppression threshold.
MaxSTm	Maximum suppression time.
MaxP	Maximum penalty value.
Restart	The default penalty value on the interface.

Related commands

Command	Description
dampening	Enable the ip event dampening function.
clear counters	Clear the interface counters.
show dampening interface	Show the statistical information of the ip event dampening function on all interfaces.

1.2.3 show ip community-list

Use **show ip community-list** command to view the community list.

show ip community-list [*community-list-number* | *community-list-name*]

Parameter description

Parameter	Description
community-list-number	Number of the community list.
community-list-name	Name of the community list.

Default configuration None

Command mode Privileged EXEC mode

Usage guidelines This command shows the information on the community list.

Examples

```
DES-7200# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

Related commands

Command	Description
match community	Match the route community.
set comm-list delete	Delete the community attribute in the BGP routes.

1.2.4 show ip prefix-list

Use **show ip prefix-list** to view the prefix list or the entries.

show ip prefix-list [*prefix-name*]

Parameter description

Parameter	Description
prefix-name	Name of the prefix list.

Default The configuration information of all the prefix lists is

configuration	displayed by default.
Command mode	Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.
Usage guidelines	If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples	`DES-7200# show ip prefix-list`
	`ip prefix-list name : test`
	`seq pre: 2 entries`
	`seq 5 permit 192.168.564.0/24`
	`seq 10 permit 192.2.2.0/24`

1.2.5 show ip route

Use the command to view the configuration of the IP routing table.

show ip route [[**vrf** *vrf_name*] [*network* [*mask*] | **count** | *protocol* [*process-id*] | **weight**]]

Parameter description

Parameter	Description
vrf *vrf_name*	(Optional) Show the route information of the VRF.
network	(Optional) Show the route information to the network.
mask	(Optional)Show the route information to the network of this mask.
count	(Optional)Show the number of existent routes. (for the ECMP/WCMP route, show one route)
protocol	(Optional) Show the route information of specific protocol.
process-id	(Optional) Routing protocol process ID.
weight	(Optional) Show the route information of non deault weight.

Default configuration	All routes are displayed by default.

Command mode

Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

This command can show route information flexibly.

Examples

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN
1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
```

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route

E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route ia: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Manage metric
Via 20.0.0.1	Next hop IP address.
VLAN 1	Forwarding interface of next hop

```
DES-7200# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
*192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF,
extern 2
```

Field	Description
Routing Descriptor Blocks	Next hop IP address, source, update time, forwarding interface, source routing protocol and type of route information

```
DES-7200# show ip route count
--------- route info ----------
the num of active route: 5

DES-7200# show ip route weight
------------[distance/metric/weight]-----------
S    23.0.0.0/8 [1/0/2] via 192.1.1.20
S    172.0.0.0/16 [1/0/4] via 192.0.0.1
```

1.2.6 show ipv6 prefix-list

Use this command to show the information about the IPv6 prefix list or its entries.

show ipv6 prefix-list [prefix-name]

Parameter description

Parameter	Description
prefix-name	Name of the IPv6 prefix list.

Default configuration

The configuration information of all the IPv6 prefix lists is displayed.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, route protocol configuration mode, route map configuration mode

Usage guideline

If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
DES-7200# show ipv6 prefix-list
Ipv6 prefix-list p6 : 2 entries
permit 13::/20
```

1.2.7 show ip route summary

Use this command to show the statistical information about one routing table.

show ip route [**vrf** *vrf_name*] **summary**

Use this command to show the statistical information about all routing tables.

show ip route summary all

Parameter description

Parameter	Description
vrf-name	VRF name

Default configuration

N/A

Command mode

Privileged user mode

Usage guideline	N/A
Examples	N/A

1.2.8 show ipv6 route

Use the command to view the configuration of the IPv6 routing table.

show ipv6 route [vrf *vrf-name***]** [[*network* / *prefix-length*] | **summary** | *protocol***| weight**]

Parameter description

Parameter	Description
network	(Optional) Show the route information to the network.
vrf-name	VRF name.
summary	(Optional)Show the classified statistics of the number of ipv6 routes.
protocol	((Optional) Show the route information of specific protocol.
weight	(Optional) show the non-default-weight routes only.

Default configuration	All routes are displayed by default.
Command mode	Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.
Usage guidelines	This command can show route information flexibly.

Examples

The following is the output of this command:

```
DES-7200(config)# show ipv6 route
IPv6 routing table name is Default(0) global scope - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
```

```
summary
O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF
external type 1, OE2 - OSPF external type 2
 ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external
type 2
      [*] - NOT in hardware forwarding table
L     ::1/128  via Loopback, local host
C     10::/64  via Loopback 1, directly connected
L     10::1/128  via Loopback 1, local host
S     20::/64  [20/0] via 10::4, Loopback 1
L     FE80::/10  via ::1, Null0
C     FE80::/64  via Loopback 1, directly connected
L   FE80::2D0:F8FF:FE22:33AB/128  via Loopback 1, local
host
```

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route ia: IS-IS area internal route
20::/64	Network address and mask of the destination network
[1/0]	Manage metric
Via 10::4	Next hop IP address.
00:00:06	Survival time of the protocol route
VLAN 1	Forwarding interface of next hop

Related commands

Command	Description
ipv6 route	Configure the ipv6 static route.

1.2.9 show route-map

Use the command to view the configuration of the route map in the privileged mode.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
route-map-name	(Optional) Show the configuration information of the specified the route map.

Default configuration

The configuration information of all the route maps is displayed.

Command mode

Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

Examples

```
DES-7200# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
```

Field	Description
route-map	Name of the route map.
Permit	The route map contains the **permit** keyword.
sequence 10	Sequence number of the route map.

Match clauses	Set the matching rule. Whether to perform the **set** operation depends on the **permit** or **deny** keyword in the route map.
Set clauses	Set the operation when the rule is matched.

2 RIP Commands

2.1 Configuration Related Commands

2.1.1 address-family (RIP)

Use this command to set the RIP protocol in the address family configuration sub-mode. The **no** form of this command removes the address family sub-mode.

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf-name*

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF name associated with the sub-mode command.

Default configuration

The address family of the RIP protocol is not configured.

Command mode

Route configuration mode.

Usage Guidelines

You can use the **address-family** command to enter the address family configuration sub-mode. The prompt is **(config-router-af)#**. When you specify the VRF associated with the sub-mode for the first time, the RIP instance corresponding to the VRF will be created. In the sub-mode, you can configure the VRF RIP routing settings.

To remove the address family sub-mode and return to the route configuration mode, execute the **exit-address-family** or **exit** command.

Examples

Create a VRF with the name of vpn1 and create its RIP instance.

```
DES-7200(config)# ip vrf vpn1
DES-7200(config-vrf)# exit
DES-7200(config)# interface fastEthernet 1/0
DES-7200(config-if-FastEthernet 0/1)# ip vrf forwarding vpn1
DES-7200(config-if-FastEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
DES-7200(config)# router rip
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router)# network 192.168.1.0
DES-7200(config-router)# exit-address-family
```

Related commands

Command	Description
exit-address-family	Exit the address family configuration sub-mode.
ip vrf	Create a VRF.

2.1.2 auto-summary (RIP)

Use this command to enable the automatic summary of RIP routes. The **no** form of this command disables the function.

auto-summary

no auto-summary

Parameter description

N/A.

Default configuration

Enabled.

Command mode

Routing process configuration mode.

Usage guidelines

The automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classful network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.

The automatic RIP route summary improves the flexibility

and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly.

Advertising summarized route is more efficient than individual routes in light of the following factors:

- The summarized route is always processed preferentially in querying the RIP database.
- Any sub-route is ignored in querying the RIP database, reducing the processing time.
- Sometimes, there is a need to learn the specific sub-routes instead of the summarized route. Here it is required to disable the automatic route summary function. Only when the RIPv2 is configured, however, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

Examples

The configuration example below disables the automatic route summary of the RIPv2.

```
DES-7200 (config)# router rip
DES-7200 (config-router)# version 2
DES-7200 (config-router)# no auto-summary
```

Related commands

Command	Description
version	Define the RIP software version: v1 or v2. Both v1 and v2 are supported by default.

2.1.3 bdf all-interfaces

Use this command to enable the BDF on all RIP interfaces. The **no** form of this command restores it to the default setting.

bdf all-interfaces

no bdf all-interfaces

Default Disabled.

Command mode Routing process configuration mode.

Usage guidelines	With the BFD function enabled on the RIP, one BFD session will be established for the RIP routing information source (the source address of the RIP routing for updating the packets). Once the BFD neighbor fails, the RIP routing information directly will enter the invalid status and join the routing forwarding no more. When establishing the BFD neighbor detection mechanism for the RIP protocol, the source addresses of the two devices that join the RIP running must be in the same segment in order to establish the BFD session between neighbors. You can also use the interface configuration mode command **ip rip bfd** [**disable**] to enable or disable the BFD function on the specified interface, which takes precedence over the command **bfd all-interfaces** in the routing process configuration mode.
Examples	N/A

Related commands

Command	Description
route ip	Create the RIP routing process and enter into the routing process configuration mode.
ip rip bfd [disable]	Enable or disable the BFD on the specified RIP interfaces.

2.1.4 default-information originate(RIP)

Use this command to generate a default route in the RIP process. The **no** form of this command deletes the generated default route.

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

Parameter description

Parameter	Description
always	(Optional) Enable RIP to generate the default route, no matter whether the default route exists or not.

metric *metric-value*	(Optional) The original metric value of the default route, in the range of 1-15.
route-map *map-name*	(Optional) Name of the associated route-map. Route-map is not associated by default.

Default configuration

No default route is generated by default.

The metric value of the generated default value is 1.

Command mode

Routing process configuration mode.

Usage guidelines

By default, RIP will not notify the default route outside, if there is no default route in the routing table. Use the **default-information originate** routing process configuration command to notify the neighbor of the default route.

With the parameter **always** configured, no matter whether the default route exists in the RIP routing process or not, the default route will be notified to the neighbor but not shown in the local routing table. Use the **show ip rip database** command to confirm the default route generation and view the RIP routing information database.

Configure the parameter **route-map** to control the default route. For example, use the **set metric** rule to set the metric value of the default route.

The route-map **set metric** rule takes precedence over the parameter **metric** value configuration of the default route. If the parameter **metric** has not been configured, the default metric value of the default route will be adopted.

Note:

If the default route can be generated by using this command, RIP will not learn the default route notified from the neighbor.

For the default route generated by using the **ip default-network** command, the default-information originate command is still needed to add the default route to the RIP.

Examples

The configuration example below generates a default route to the RIP routing table:

	`DES-7200(config-router)# default-information originate always`

Related commands	**Command**	**Description**
	ip rip default-information	Notify the default route on an interface.
	redistribute	Redistribute the routes from one routing domain to another routing domain.

2.1.5 default-metric (RIP)

Use this command to define the default RIP metric in the route configuration mode. The **no** form of this command is used to restore it to the default value.

default-metric *metric*

no default-metric

Parameter description	**Parameter**	**Description**
	metric	Default metric in the range of 1 to 16. If the metric is greater than or equal to 16, the route is regarded unreachable.

Default configuration	The default value is 1.
Command mode	Routing process configuration mode.
Usage guidelines	This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric cannot be converted due to the incompatibility of the metric calculation mechanism of different protocols. During the conversion, therefore, it is required to redefine the metric of redistributed routes in the RIP routing domain. If there is no clear definition of metric in redistributing a routing protocol process, the RIP uses the metric defined with **default-metric**. If a clear metric is defined, this value overwrites the metric defined with **default-metric**. If this command is not configured, the default value of default-metric is 1.

Examples

In the configuration example below, the RIP routing protocol redistributes the routes learned by the OSPF routing protocol, whose initial RIP metric is set as 3.

```
DES-7200 (config)# router rip
DES-7200 (config-router)# default-metric 3
DES-7200 (config-router)# redistribute ospf 100
```

Related commands

Command	Description
redistribute	Redistribute the routes from one routing domain to another routing domain.

2.1.6 distance

Use this command to set the management distance of the RIP route. The **no** form of this command restores it to the default setting.

distance *distance* [*ip-address wildcard*]

no distance *distance* [*ip-address wildcard*]

Parameter description

Parameter	Description
distance	Management distance of a RIP route, an integer in the range of 1 to 255
ip-address	Prefix of the source IP address of the route
wildcard	Comparison bit of the IP address, where 0 means accurate matching while 1 means no comparison

Default The default value is 120.

Command mode Routing process configuration mode.

Usage guidelines	Use this command to set the management distance of the RIP route. You can use this command to create several management distances with source address prefix. When the source address of the RIP route is within the range specified by the prefix, the corresponding management distance is applied; otherwise, the route uses the management distance set by the RIP.

Examples	Set the management distance of the RIP route to **160**, and specify the management distance of the route learned from 192.168.2.1 to **123**.
	`DES-7200(config)# router rip`
	`DES-7200(config-router)# distance 160`
	`DES-7200(config-router)# distance 123 192.168.12.1 0.0.0.0`

2.1.7 distribute-list in (RIP)

Use this command to control route update for filtering in the routing process configuration mode. The **no** form of this command removes the configuration.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes on the ACL are accepted.
prefix *prefix-list-name*	Use the prefix list to filter the routes.
gateway *prefix-list-name*	Use the prefix list to filter the source of the routes.
i*nterface-type interface-number*	(Optional) Interface that the distribution list applies to

Default configuration	N/A.
Command mode	Routing process configuration mode.

Usage guidelines	To deny some specified routes, you can process all the route update packets received by configuring the route distribute control list. Without any interface specified, the system will process the route update packet received on all the interfaces.

Examples	In the following configuration example, the RIP controls and processes the routes received from the Fastethernet 0/0 port, only permitting the routes starting with 172.16.
	`DES-7200 (config)# router rip`
	`DES-7200 (config-router)# network 200.168.23.0`
	`DES-7200 (config-router)# distribute-list 10 in fastethernet 0/0`
	`DES-7200 (config-router)# no auto-summary`
	`DES-7200 (config-router)# access-list 10 permit 172.16.0.0 0.0.255.255`

Related commands

Parameter	Description
access-list	Define the ACL.
prefix-list	Define the prefix of the ACL.

2.1.8 distribute-list out (RIP)

Use this command to control route update advertisement for filtering routes in the routing process configuration mode. The **no** form of this command removes this configuration.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protoco*] [*process-id* | *process-name*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id* | *process-name*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes on the ACL are permitted.
prefix *prefix-list-name*	Use the prefix list to filter the routes.
Interface	(Optional) Interface that the route update advertisement control applies to

	protocol	(Optional) Routing protocol whose routes are selectively redistributed
	process-id	(Optional) Set the OSPF process ID when OSPF is used.
	process-name	(Optional) Set the ISIS process name when ISIS is used.

Default configuration

No route update advertisement is configured.

Command mode

Routing process configuration mode.

Usage guidelines

No optional parameters means the route update advertisement applies to all ports. Interface option means the control applies to only the specified port. Protocol option means the route update advertisement control applies to only the specific route process.

Examples

In the following configuration example, the RIP routing process only advertises the 192.168.12.0/24 route.

```
DES-7200 (config)# router rip
DES-7200 (config-router)# network 200.4.4.0
DES-7200 (config-router)# network 192.168.12.0
DES-7200 (config-router)# distribute-list 10 out
DES-7200 (config-router)# version 2
DES-7200 (config-router)#access-list 10 permit
192.168.12.0 0.0.0.255
```

Related commands

Parameter	Description
access-list	Define the ACL.
prefix-list	Define the prefix of the ACL.
redistribute	Configure route redistribution.

2.1.9 exit-address-family

Use this command to exit the address family configuration mode.

exit-address-family

Parameter description	N/A.
Default configuration	N/A.
Command mode	Address family configuration mode.
Usage guidelines	Use this command to exit the address family configuration mode. The abbreviation of this command is **exit** .

Examples	Following example shows how to enter or exit the address family configuration mode:
	`DES-7200(config-router)# address-family ipv4 vrf vpn1`
	`DES-7200(config-router-af)# exit-address-family`

Related commands

Parameter	Description
address-family	Enter the address family configuration sub-mode

2.1.10 graceful-restart(RIP)

Use this command to configure the RIP graceful restart (GR) function on a device. The **graceful-restart grace-period** command is used to display the configured GR grace period parameter and enable the RIP GR function. The **no** form of this command is used to restore the default configuration.

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter description

Parameter	Description
graceful-restart	Enable the GR function.
grace-period	Display the configured grace-period (optional).
grace-period	Indicate the user-defined GR period (optional). The default value is the smaller of either twice the update time

	or 60s. The value is in the range of 1s to 1,800s.

Default configuration

Disabled.

Command mode

Routing process configuration mode

Usage guidelines

The GR function is configured on the basis of RIP instances. Different GR parameters can be configured for different RIP instances.

GR period is the longest time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the pre-GR state. When the period is due, the RIP exits the GR state and starts normal RIP operation. The **graceful-restart grace-period** command allows you to explicitly modify the grace period. Note: Make sure that GR is completed before the RIP route is validated and after an RIP route update cycle elapses. If the value is incorrectly configured, you cannot ensure that data is transferred uninterruptedly during the GR period. For example, if the grace period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not reinformed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in network data transmission interruption. Therefore you are not suggested to change the grace period unless there is an obvious necessity. If you need to change it, configure the **timers basic** command to make sure the grace period is longer than the route update cycle and shorter than the time when the route is unavailable.

Caution

During the RIP GR period, keep the stable network environment.

Examples

The configuration example below enables the RIP GR function and configure the grace period of the GR function:.

```
DES-7200(config)# router rip
DES-7200(config-router)# graceful-restart grace-period 90
```

Related commands

Command	Description
timers basic	Configure RIP timers.

2.1.11 ip rip authentication key-chain

Use this command to enable the RIP authentication and specify the keychain used for RIP authentication in the interface configuration mode. The **no** form of this command is used to delete the specified keychain.

ip rip authentication key-chain *name-of-keychain*

no ip rip authentication key-chain

Parameter description

Parameter	Description
name-of-keychain	Name of the keychain used for RIP authentication

Default configuration

The keychain is not associated by default.

Command mode

Interface configuration mode.

Usage guidelines

If the keychain is specified in the interface configuration mode but not defined with the **key chain** global configuration command, the RIP authentication will not be performed.

The RIPv1 does not support authentication but the RIPv2 does.

Examples

The configuration example below enables the RIP authentication on the fastEthernet 0/1 with the associated keychain is ripchain.

```
DES-7200 (config)#interface fastEthernet 0/0
DES-7200 (config-if-FastEthernet 0/1)#ip rip authentication key-chain ripchain
```

Related

Command	Description

ip rip authentication mode	Define the RIP authentication mode.
ip rip authentication text-password	Enable the RIP authentication, and set the password string of RIP plaintext authentication. The RIP packets authentication is supported by the RIPv2 only.
ip rip receive version	Define the version of RIP packets received on the interface.
ip rip send version	Define the verion of RIP packets sent on the interface.
key chain	Define the keychain and enter into the keychain configuration mode.

2.1.12 ip rip authentication mode

Use this command to define the RIP authentication mode in the interface configuration mode. The **no** form of this command is used to restore it to the default RIP authentication mode.

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

Parameter description

Parameter	Description
text	Enable plaintext authentication.
md5	Enable MD5 authentication.

Default configuration It is the plaintext authentication by default.

Command mode Interface configuration mode.

Usage guidelines	To exchange RIP routing information directly, all devices must have the same RIP authentication mode. Otherwise, the RIP packet exchange will fail. If the plaintext authentication is adopted, but the password string of the plaintext authentication or the associated keychain is not configured or the associated keychain is not configured in practice, the authentication is not performed in this case. In the same way, if the MD5 authentication is adopted, but the associated keychain is not configured or the associated keychain is not configured in practice, the authentication is not performed as well. The RIPv1 does not support RIP authentication but the RIPv2 does.

Examples	The configuration example below configures the RIP authentication mode on the fastEthernet 0/1 as md5.
	`DES-7200 (config)#interface fastEthernet 0/1`
	`DES-7200 (config-if-FastEthernet 0/1)# ip rip authentication mode md5`

Related commands

Command	Description
ip rip authentication key-chain	Enable the RIP authentication and specify the keychain used for the RIP authentication. Only the RIPv2 supports authentication.
ip rip authentication text-password	Enable the RIP authentication, and set the password string of RIP plaintext authentication. The RIP packets authentication is supported by the RIPv2 only.
key chain	Define the keychain and enter into the keychain configuration mode

2.1.13 ip rip authentication text-password

Use this command to set the password string of RIP plaintext authentication. The **no** form of this command is used to remove the password string.

ip rip authentication text-password *password-string*

no ip rip authentication text-password

Parameter description

Parameter	Description
password-string	Password string of the plaintext

		authentication, in the length of 1-16 bytes.

Default configuration	No password string of RIP plaintext authentication is configured by default.
Command mode	Interface configuration mode.
Usage guidelines	To enable the RIP plaintext authentication, the password string can be configured directly by using this command, or can be obtained by associating with the key chain. The latter takes the precedence over the former one. The RIPv1 does not support RIP authentication but the RIPv2 does.

Examples	The configuration example below enables the RIP plaintext authentication on the fastEthernet 0/1 and sets the password string as hello:
	`DES-7200(config)#interface fastEthernet 0/1`
	`DES-7200(config-if-FastEthernet 0/1)# ip rip authentication text-password hello`

Related commands	**Command**	**Description**
	ip rip authentication mode	Define the RIP authentication mode.
	ip rip authentication key-chain	Enable the RIP authentication and specify the keychain used for the RIP authentication. Only the RIPv2 supports authentication.

2.1.14 ip rip bdf

Use this command to enable or disable the BFD on the specifed RIP interface. The **no** form of this command is used to remove the setting on the interface..

ip rip bfd [**disable**]

no ip rip bfd

Parameter description	**Parameter**	**Description**
	disable	Disable the BFD function on the

		specified RIP interface.

Default configuration	N/A
Command mode	Interface configuration mode.
Usage guidelines	The command **ip rip bfd** in the interface configuration mode takes precedence over the **bfd all-interfaces** command in the routing process configuration mode. You can use this command to enable the BFD on the specified interface according to the actual environment, also can use the command **bfd all-interfaces** in the RIP process configuration mode to enanble the BFD function on all RIP interfaces and use the command **ip rip bfd disable** to disable the BFD on the specified interface.
Examples	N/A

Related commands

Command	Description
route ip	Create the RIP routing process and enter into the routing process configuration mode.
bdf all-interfaces	Enable the BFD on all RIP interfaces.

2.1.15 ip rip default-information

Use this command to notify a specified interface of the RIP default route. The **no** form of this command is used to cancel the notification of the default route.

ip rip default-information {**only** | **originate**} [**metric** *metric-value*]

no ip rip default-information

Parameter description

Parameter	Description
only	Notify the default route, rather than other routes.
originate	Notify the default route and other routes.
metric	Specify the metric value of the default

metric-value	route, in the range of 1-15.

Default configuration

No default route is configured by default. The default metric is 1.

Command mode

Interface configuration mode.

Usage guidelines

After configuring this command on a specified interface, a default route will be notified through this interface. If the **ip rip default-information** command in the interface configuration mode and the **default-information originate** command in the RIP process are configured at the same time, it only notifies the interface of the default route.

Note:

1. RIP will not learn the default route notified by the neighbor, if the **ip rip default-information** command does not configured on an interface. If the default route has been learned, it will be removed till the timer expires.
2. The **ip rip default-information** command configuration on the interface can not be triggered and updated immediately, and will be notified on the next timed update message.

Examples

The configuration example below creates a default route which is notified on the interface ethernet0/1 only:

```
DES-7200(config)#interface ethernet 0/1
DES-7200(config-if-Ethernet 0/1)#ip rip
default-information only
```

Related commands

Command	Description
default-information originate	Originate the default route in the RIP process.

2.1.16 ip rip receive enable

Use this command to receive RIP packets on the interface. The **no** form of this command prohibits receiving RIP packets on the interface .

ip rip receive enable

no ip rip receive enable

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	To prevent from receiving RIP packets on the interface, use the **no** form of this command in the interface configuration mode. To this end, you must configure this command on the interface. The **default** form of this command restores it to the default value.

Examples	Prohibit from receiving RIP packets on the fastEthernet 0/1.
	`DES-7200 (config)# interface fastEthernet 0/1`
	`DES-7200 (config-if-FastEthernet 0/1)# no ip rip receive enable`

Related commands

Parameter	Description
ip rip send enable	Enable sending RIP packets on the interface.
passive-interface	Set the interface to a passive interface.

2.1.17 ip rip receive version

Use this command to define the version of RIP packets received on the interface in the interface configuration mode. The **no** form of this command is used to restore it to the default value.

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter description

Parameter	Description
1	(Optional) Receive only RIPv1 packets.
2	(Optional) Receive only RIPv2 packets.

Default configuration	The default behavior depends on the configuration with the **version** command.
Command mode	Interface configuration mode.
Usage guidelines	This command overwrites the default configuration of the **version** command. It allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If there is no parameter when the command is configured, the receiving behavior will depend on the configuration of the version.
Examples	The configuration example below enables receiving both RIPv1 and RIPv2 packets on the fastEthernet 0/1 interface. `DES-7200 (config)#`**`interface`** *`fastEthernet 0/1`* `DES-7200 (config-if-FastEthernet 0/1)#` **`ip rip receive version 1 2`**

Related commands

Command	Description
version	Define the default version of the RIP packets received/sent on the interface.

2.1.18 ip rip send enable

Use this command to enable sending RIP packets on the interface. The **no** form of this command disables sending RIP packets on the interface.

ip rip send enable

no ip rip send enable

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Interface configuration mode.

Usage guidelines	To prevent from sending RIP packets on the interface, use the **no** form of this command in the interface configuration mode. To this end, you must configure this command on the interface. The **default** form of this command can restore it to the default value.

Examples	Prohibit from sending RIP packets on the fastEthernet 0/1.
	`DES-7200 (config)# interface fastEthernet 0/1`
	`DES-7200 (config-if-FastEthernet 0/1)# no ip rip send enable`

Related commands

Parameter	Description
ip rip receive enable	Enable receiving RIP packets on the interface.
passive-interface	Set the interface to a passive interface.

2.1.19 ip rip send supernet-routes

Use this command to enable sending the RIP supernet-routes on the specified interface The **no** form of this command disables sending the RIP supernet-routes on the specified interface.

ip rip send supernet-routes

no ip rip send supernet-routes

Default configuration	Enabled
Command mode	Interface configuration mode.

Usage guidelines

When the RIPv1 router is monitoring the response message from the RIPv2 router, if the supernet routing information is monitored, an incorrect route is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, it needs to use the **no** form of this command on the RIPv2 router to disable advertising the supernet-routes on the corresponding interface. This command only takes effect on the interfaces with this command configured.

Note

This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet-routes.

Examples

The configuration example below disables sending RIP supernet-routes on the fastEthernet 0/1 interface.

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# no ip rip send supernet-routes
```

Related commands

Command	Description
version	Define the RIP version
ip rip send enable	Enable or disable sending the RIP packets on the interface.

2.1.20 ip rip send version

Use this command to define the version of the RIP packets sent on the interface in the interface configuration mode. The **no** form of this command is used to restore it to the default value.

ip rip send version [**1**] [**2**]

no ip rip send version

Parameter description

Parameter	Description
1	(Optional) Send only RIPv1 packets.
2	(Optional) Send only RIPv2 packets.

Default configuration

The default behavior depends on the configuration with the **version** command.

Command mode	Interface configuration mode.
Usage guidelines	This command overwrites the default configuration of the **version** command. It allows RIPv1 and RIPv2 packets to be sent on the interface at the same time. If there is no parameter when the command is configured, the receiving behavior will depend on the configuration of the version.

Examples	The configuration example below enables sending both RIPv1 and RIPv2 packets on the fastEthernet 0/1 interface.
	`DES-7200 (config)# interface fastEthernet 0/1`
	`DES-7200 (config-if-FastEthernet 0/1)# ip rip send version 1 2`

Related commands

Command	Description
version	Define the default version of the RIP packets received/send on the interfaces.

2.1.21 ip rip v2-broadcast

Use this command to send RIPv2 pakcets in broadcast form rather than in multicast form. The **no** form of this command restores it to the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter description	N/A.
Default configuration	The default depends on the configuration of the **version** command.
Command mode	Interface configuration mode.

Usage guidelines	This command overwrites the default of the **version** command. This command only affects the behavior of sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packets to be sent on the interface simultaneously. Without parameters specified, which packets will be received depends on the **version** setting.

Examples	Send RIPv2 packets in the broadcast mode on the fastEthernet 0/1 interface.
	`DES-7200(config)# interface fastEthernet 0/1`
	`DES-7200(config-if-FastEthernet 0/1)# no ip rip split-horizon`

Related commands

Parameter	Description
version	Define the default version of the RIP packets received and sent on the interface.

2.1.22 ip rip split-horizon (RIP)

Use this command to enable split horizon in the interface configuration mode. The **no** form of this command disables the function.

ip rip split-horizon

no ip rip split-horizon

Parameter description	N/A.
Default configuration	By default, this function is enabled on all interfaces.
Command mode	Interface configuration mode.
Usage guidelines	When multiple devices are connected to the IP broadcast network using a distance vector routing protocol, it is required to use the split horizon mechanism to prevent loop. The split horizon prevents the device from advertising some routing information from the interface that learns that information, which optimizes the routing

information exchange between multiple devices.

For non-broadcast multi-path access network (such as frame relay and X.25), however, the split horizon may cause some devices unable to learn all routing information. The split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for the split horizon issue.

The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, execute the **show ip rip** command. This function makes no influence on the neighbor defined with the **neighbor** command.

Examples

The configuration example below disables the RIP split horizon function on the interface fastethernet 0/0.

```
DES-7200 (config)# interface fastethernet 0/0
DES-7200 (config-if)# no ip rip split-horizon
```

Related commands

Command	Description
neighbor (RIP)	Define a neighbor.
validate-update-source	Enable the source address authentication of the RIP route update message.

2.1.23 ip rip summary-address

Use this command to enable port-level convergence in the interface configuration mode. The **no** form of this command disables the convergence of the specified address or subnet.

ip rip summary-address *ip-address ip-network-mask*

no ip rip summary-address *ip-address ip-network-mask*

Parameter description

Parameter	Description
ip-address	IP addresses to be converged
ip-network-mask	Subnet mask of the specified IP address to be converged

Default The RIP routes are automatically converged to the

configuration	classful network edge.
Command mode	Interface configuration mode.
Usage guidelines	This command converges an address or subnet on a specified port. RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.

Examples	The following configuration example disables the route convergence function of the RIPv2. The port convergence is configured so that the fastEthernet 0/1 advertises the converged route 172.16.0.0/16.
	`DES-7200 (config)# interface fastEthernet 0/1`
	`DES-7200 (config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0`
	`DES-7200 (config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0`
	`DES-7200 (config)# router rip`
	`DES-7200 (config-router)# network 172.16.0.0`
	`DES-7200 (config-router)# version 2`
	`DES-7200 (config-router)# no auto-summary`

Related commands

Parameter	Description
auto-summary	Enable the automatic convergence of RIP routes.

2.1.24 ip rip triggered

Use this command to enable triggered RIP for the link on demand in the interface configuration mode. The **no** form of this command is used to disable triggered RIP.

ip rip triggered

ip rip triggered retransmit-timer *timer*

ip rip triggered retransmit-count *count*

no ip rip triggered

no ip rip triggered retransmit-timer

no ip rip triggered retransmit-count

Parameter description

Parameter	Description
retransmit-timer *timer*	Configure the interval at which the Update Request and Update Response packets are retransmitted. The value is in the range of 1s to 3600s, and 5s by default.
retransmit-count *count*	Configure the maximum times that the Update Request and Update Response packets are retransmitted. The value is in the range of 1 to 3600, and is 36 by default.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for the link on demand.

With the TRIP enabled, RIP no longer sends route updates regularly and sends route updates to the WAN interface only if:

- Update Request packets are received.
- RIP routing information is changed.
- Interface state is changed.
- The router is started.

As RIP regular update is disabled, the confirmation and retransmission mechanism is needed to ensure update packets are sent and received successfully over the WAN. The **retransmit-timer** and **retransmit-count** commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.

2. The function can be enabled when a) the interface has only one neighbor, or b) there are multiple neighbors but they interact using unicast packets. You are suggested to enable the function for link layer protocols such as PPP, frame relay, and X.25.
3. You are suggested to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might left.

Caution

4. Make sure the function is enabled on all routers on the same link; otherwise the function will be invalidated and the routing information cannot be exchanged correctly.
5. The function cannot be enabled at the same time with BFD and RIP functions.
6. To enable the function, make sure the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.
7. If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source address check function (validate-update-source) is enabled.

Examples

The following configuration example enables triggered RIP and specifies the retransmission interval and maximum retransmission times to 10s and 18 respectively for Update Request and Update Response packets.

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip rip triggered
DES-7200(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10
DES-7200(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18
```

Related commands

Parameter	Description
show ip rip database	Show the summarized routing information of the RIP database.
show ip rip interface	Show the RIP interface information.
ip rip split-horizon	Configure the RIP split horizon.

2.1.25 neighbor (RIP)

Use this command to define a RIP neighbor in the routing process configuration mode. The **no** form of this command is used to delete the neighbor.

neighbor *ip-address*

no neighbor

Parameter description

Parameter	Description
ip-address	IP address of the neighbor.

Default configuration

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

By default, the RIPv1 works with the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 works with the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, execute the **passive-interface** command in the routing process configuration mode to configure the related interfaces as passive interface and then define only some neighbor to be able to receive the routing information. This command does not affect the receiving of RIP messages. Once restart, the interface who is set to passive will not send request message.

Examples

The configuration example below defines two neighbors.

```
DES-7200 (config)# router rip
DES-7200 (config-router)# network 192.168.12.0
```

```
DES-7200 (config-router)# network 172.16.0.0
```

Related commands -

2.1.26 network (RIP)

Use this command to define the list of networks to be advertised in the RIP routing process in the routing process configuration mode. The **no** form of this command is used to delete the defined network.

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter description

Parameter	Description
network-number	Number of the directly-connected network. This network number is a natural network number. All interfaces whose IP addresses belong to that natural network can send/receive the RIP packets.
wildcard	Define the IP address comparing bit: 0 refers to accurate matching, 1 refers to no comparing.

Command mode Routing process configuration mode.

Usage guidelines

The *network-number* and *wildcard* parameter can be configured simultaneously to make the IP address for the interface within the address range join the RIP running.

Only when the IP address of an interface is in the network list defined for the RIP, the RIP route update messages can be received and sent on the interface.

Examples

The following example defines two network numbers associated with the RIP process.

```
DES-7200 (config)# router rip
DES-7200 (config-router)# network 192.168.12.0
DES-7200 (config-router)# network 172.16.0.0
```

Related commands

2.1.27 offset-list(RIP)

Use this command to increase the metric value of receiving or sending route. The **no** form of this command deletes the specified offset list.

offset-list *access-list-number* {**in** | **out**} *offset* [*interface-type interface-number*]

no offset-list *access-list-number* {**in** | **out**} *offset* [*interface-type interface-number*]

Parameter description

Parameter	Description
access-list-number	ACL number
in	Modify the metric of the routes received by ACL.
out	Modify the metric of the routes sent by ACL.
offset	Change of the metric value
interface-type	Interface that the ACL applies to
interface-number	Interface that the ACL applies to

Default configuration

The offset is not specified.

Command mode

Routing process configuration mode.

Usage guidelines

If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

Examples

Increase the metric of the RIP routes by 7 in the range specified by ACL 7.

```
DES-7200 (config-router)# offset-list 7 out 7
```

Increase the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastethernet 0/1.

```
DES-7200 (config-router)# offset-list 7 in 7
DES-7200 (config-router)# offset-list 8 in 7 fastethernet
```

0/1

2.1.28 output-delay

Use this command to modify the delay to send the RIP update packets. The **no** form of this command removes the configuration.

output-delay *delay*

no output-delay

Parameter description

Parameter	Description
delay	Delay to send the RIP update packets in the range from 8 ms to 50 ms.

Default configuration

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

Normally, the size of a RIP update packet is 512 Kbytes including 25 routes. If the number of the update routes is larger than 25, the routes will be sent in several packets as fast as possible.

However, when a high-speed device sends a large amount of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Examples

Set the delay to send the RIP update packets to 30 ms.

```
DES-7200(config)# router rip
DES-7200(config-router)# output-delay 30
```

2.1.29 passive-interface

Use this command to set an interface to a passive interface. The **no** form of this command removes this configuration.

passive-interface {**default** | *interface-type interface-num*}

no passive-interface {**default** | *interface-type interface-num*}

Parameter description

Parameter	Description
Default	Set the interface to a passive interface.
interface-type interface-num	Interface type and number

Default configuration

By default, ports are set to the non passive mode.

Command mode

Routing process configuration mode.

Usage guidelines

The **passive-interface default** command sets all interfaces to the passive mode. You can use **no passive-interface** *intface-type interface-num* to set the specified interface to the non-passive mode.

When you enable receiving and sending RIP messages on the interface with the **ip rip send enable** and **ip rip receive enable** commands, this command sets the interface to the passive mode. Consequently, receiving RIP update messages rather than sending RIP update messages is enabled on the interface. However, the **ip rip send enable** and **ip rip receive enable** commands determine whether the messages can be sent or received.

Examples

Set all interfaces to the passive mode and then set ethernet0/1 to the non-passive mode.

```
DES-7200(config-router)# passive-interface default
DES-7200(config-router)# no passive-interface gigabitEthernet 0/1
```

Related commands

Command	Description
ip rip receive enable	Enable receiving RIP packets on the interface.
ip rip send enable	Enable sending RIP packets on the interface.

2.1.30 redistribute (RIP)

Use this command to redistribute external routes in the route configuration mode. The **no** form of this command cancels the redistribution of external routes.

redistribute {**bgp**| **isis** [*process-name*] |**ospf** <*1-65535*>| **connected** | **static**} [**metric** *value*] [**route-map** *route-map-name*][**match internal** | **external** *type* | **nssa-external** *type*]

no redistribute {**bgp** | **isis** [*process-name*] | **ospf** <*1-65535*> | **connected** | **static**} [**metric** *value*] [**route-map** *route-map-name*][**match internal** | **external** *type* | **nssa-external** *type*]

Parameter description

Parameter	Description
bgp | isis | ospf | connected | static	Specify the route redistribution protocol.
metric	Set the metric of the route to be redistributed.
route-map	Set the redistribution rule.
match	Redistribute OSPF-type routes.
<*1-65535*>	Number of an OSPF instance

Default

By default:

All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF.

The routes of Level-2 sub-types of the instance are redistributed when you configure ISIS redistribution.

All the routes of the protocol are redistributed for other routing protocols.

The metric of the redistributed routes is 1 by default.

The route-map is not associated.

Command mode

Routing process configuration mode.

Usage guidelines

This command redistributes external routes.

It is not necessary to convert the metric of one routing protocol into that of another routing protocol for route distribution, since different routing protocols use different metric measurement methods. The RIP protocol calculates metric on hop, the OSPF on bandwidth. So their metrics are not comparable. However, a symbolic metric must be set for route redistribution. Otherwise, route redistribution will fail.

When you configure ISIS routes redistribution without the **level** parameter, only level-2 routes are redistributed by default. If the redistribution configuration is initialize with **level** parameter, then all routes with **level** configured are redistributed.

When you configure redistributing OSPF routes without the **match** parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The **no** form of this command restores the setting to the default value.

Note:

The redistribute command cannot redistribute the default route of other protocol to the RIP process. To this end, execute the **default-information originate** command.

Examples

Redistribute static routes.

```
DES-7200(config-router)# redistribute static
```

Related commands

Command	Description
default-metric *metric*	Set the default metric of the route to be redistributed.

2.1.31 router rip

Use this command to create the RIP routing process and enter into the routing process configuration mode. The **no** form of this command is used to delete the RIP routing process.

router rip

no router rip

Parameter description	N/A.
Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	One RIP routing process must be defined with one network number. If a dynamic routing protocol is running on asynchronous lines, execute **async default routing** on the asynchronous interface.
Examples	The configuration example below describes how to create the RIP routing process and enter into the routing process configuration mode. `DES-7200 (config)# router rip`

Related commands

Command	Description
network (RIP)	Define the network number of the RIP process.

2.1.32 timers basic

Use this command to adjust the RIP clock in the routing process configuration mode. The **no** form of this command is used to restore it to the default.

timers basic *update invalid flush*

no timers basic

Parameter description

Parameter	Description
update	Route update time, in seconds. The *update* keyword defines the period at which the device sends route update messages. Once an update message is received, the "Invalid" and "Flush" clocks reset. By default, a route update message is sent every 30 seconds.
invalid	Route invalid period, in seconds, starting from the last valid update

	message. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update message is received within the route invalid period, the related route becomes invalid and enters into the "invalid" state. If a update message is received within the period, the clock resets. By default the Invalid period is 180s.
flush	Route flushing period, in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush period is 120 s.

Default configuration

By default, the update time is 30s, invalid time is 180s and flushing time is 120 s.

Command mode

Routing process configuration mode.

Usage guidelines

Adjusting the above clocks may speed up the routing protocol convergence and fault recovery. The devices connected with the same network must have the same RIP clock settings. The adjustment of RIP clocks is not recommended unless otherwise necessary.

To check the current RIP clock parameters, execute the **show ip rip** command.

Examples

The configuration example below enables the RIP update message to be sent every 10 seconds. If no update message is received within 30s, the related routes become invalid and enter into the invalid status. When another 90s elapses, they will be cleared.

```
DES-7200 (config)# router rip
DES-7200 (config-router)# timers basic 10 30 90
```

Note that the small settings of clocks on low-speed links may cause some risks, because numerous update

	messages may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2Mbps to reduce the convergence time of routes.

2.1.33 validate-update-source

Use this command to validate the source address of the received RIP route update message in the routing process configuration mode. The **no** form of the command disables the source address validation.

validate-update-source

no validate-update-source

Default configuration	Enabled.
Command mode	Routing process configuration mode.
Usage guidelines	It is possible to validate the source address of the RIP route update message. The validation aims to ensure the RIP routing process receives only the route updates from the same IP subnet neighbor. Disabling split-horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the **validate-update-source** command in the routing process configuration mode. In addition, for the **ip unnumbered** interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the routing process configuration command **validate-update-source**.

Examples	The configuration example below disables the message source address validation.
	`DES-7200 (config)# router rip`
	`DES-7200 (config-router)# no validate-update-source`

Related	**Command**	**Description**

ip split-horizon	Enable split horizon.
ip unnumbered	Define the IP unnumbered interface
neighbor (RIP)	Define a neighbor.

2.1.34 version (RIP)

Use this command to define the RIP version in the routing process configuration mode. The **no** form of this command is used to restore it to the default.

version {**1** | **2**}

no version

Parameter description

Parameter	Description
1	Define the RIP version 1.
2	Define the RIP version 2.

Default configuration

By default, the route update messages of the RIPv1 and RIPv2 are received, but those of the RIPv1 is send only.

Command mode

Routing process configuration mode.

Usage guidelines

This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

Examples

The configuration example below configures the RIP version 2.

```
DES-7200 (config)# router rip
DES-7200 (config-router)# version 2
```

Related commands

Command	Description
ip rip receive version:	Define the version of RIP packets received on the interface.
ip rip send version	Define the version of RIP packets sent on the interface.
show ip rip	Show RIP information.

2.2 Showing Related Command

2.2.1 show ip rip

Use this command to show the RIP information.

show ip rip [**vrf** *vrf-name*]

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the vrf and display the basic information of the corresponding RIP instance.

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

It is used to show the three timers, routing distribution, routing re-distribution status, interface RIP version, RIP interface and network range, metric, distance and so on of the RIP routing protocol process quickly. If vrf is specified, display the name of VRF and VRF-id.

Examples

In the configuration example below, the basic information of the RIP routing protocol is displayed, such as the refresh time, management distance, etc.

```
DES-7200#show ip rip
Routing Protocol is "rip"
  Sending updates every 10 seconds, next due in 4 seconds
  Invalid after 20 seconds, flushed after 10 seconds
  Outgoing update filter list for all interface is: not
set
  Incoming update filter list for all interface is: not
set
  Default redistribution metric is 2
  Redistributing: connected
  Default version control: send version 2, receive version
2
    Interface            Send  Recv
    FastEthernet 0/1      2     2
    FastEthernet 0/2      2     2
  Routing for Networks:
```

```
    192.168.26.0 255.255.255.0
    192.168.64.0 255.255.255.0
  Distance: (default is 50)
```

Follwoing example specifies vrf and displays the corresponding basic information of RIP instance:

```
DES-7200(config-router)# sh ip rip vrf 1
VRF 1  VRF-id:1
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 4 seconds
  Invalid after 180 seconds, flushed after 120 seconds
  Outgoing update filter list for all interface is: not
set
  Incoming update filter list for all interface is: not
set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 1, receive any
version
  Routing for Networks:
  Distance: (default is 120)
```

2.2.2 show ip rip database

Use this command to show the summary address entries in the RIP routing database.

show ip rip database [**vrf** *vrf-name*] [*network-number* {*network-mask*}]

Parameter description

Parameter	Description
vrf *vrf-name*	(Optional) Show the RIP routing information of specified VRF.
network-number	(Optional) Network number
network-mask	Subnet maskIt if the network number is specified.

Default configuration N/A.

Command mode Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the

converged address information will be deleted from the database.

Examples

In the configuration example below, all converged address entries in the RIP routing database are displayed.

```
DES-7200# show ip rip database
192.168.1.0/24    auto-summary
192.168.1.0/30    directly connected, Loopback 3
192.168.1.8/30    directly connected, FastEthernet 0/1
192.168.121.0/24    auto-summary
192.168.121.0/24    redistributed
    [1] via 192.168.2.22, FastEthernet 0/2
192.168.122.0/24    auto-summary
192.168.122.0/24
    [1] via 192.168.4.22, Serial 0/1  00:28    permanent
```

In the configuration example below, the converged address entries related with 192.168.121.0/24 in the RIP routing database are displayed.

```
DES-7200# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24    redistributed
[1] via 192.168.2.22, FastEthernet 0/1
```

In the configuration example below, show the statistical information summary of various routes in the RIP routing database.

```
DES-7200# show ip rip database count
              All    Valid   Invalid
database       5      5      0
auto-summary    5      5      0

connected      1      1      0
rip            4      4      0
```

Related commands

Command	Description
show ip rip	Show the information of the currently-running routing protocol process.

2.2.3 show ip rip external

Use this command to show the information of the external routes redistributed by the RIP protocol.

show ip rip external [**bgp** | **connected** | **isis [***process-name***] |ospf <***1-65535***>**| static] [**vrf** *vrf-name*]

Parameter description

Parameter	Description
bgp | connected | isis | ospf | static	Show the external route redistributed by the specified routing protocol (optional).
vrf vrf-name	Show the RIP external route of the specified VRF (optional)..
<*1-65535*>	Number of the OSPF instace

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Examples

The following is an example showing the direct routes redistributed by the RIP process.

```
DES-7200# show ip rip external connected
Protocol connected route:
[connected] 1.0.0.0/8 metric=0
nhop=0.0.0.0, if=2
[connected] 3.0.0.0/8 metric=0
nhop=0.0.0.0, if=16391
[connected] 4.4.0.0/16 metric=0
nhop=0.0.0.0, if=16388
[connected] 5.0.0.0/8 metric=0
nhop=0.0.0.0, if=16386
[connected] 192.168.195.0/24 metric=0
nhop=0.0.0.0, if=1
```

Related commands

Command	Description
show ip rip	Show the information of the currently running routing protocol process.

2.2.4 show ip rip interface

Use this command to show the RIP interface information.

show ip rip interface [**vrf** *vrf-name*] [*interface-type interface-number*]

Parameter description

Parameter	Description
vrf *vrf-name*	Show the RIP interface of specified VRF (optional).
[*interface-type interface-number*]	Show the specified interface type and interface number(optional).

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

This command is used to show the information about RIP interfaces. If there is no RIP interface, no information is shown.

Examples

The following is an example showing the RIP interface information.

```
DES-7200# show ip rip interface
FastEthernet 01 is down, line protocol is down
  RIP is not enabled on this interface
FastEthernet 1/0 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv2 packets only
    Send RIPv2 packets only
    Passive interface: Disabled
    Split horizon: Enabled
    V2 Broadcast: Disabled
    Multicast register: Registed
    Interface Summary Rip:
      Not Configured
    Authentication mode: Text
    Authentication key-chain: ripk1
    Authentication text-password:DES-7200
    Default-information: only, metric 5
    IP interface address:
      192.168.64.100/24
```

If the BFD has been configured for RIP, the BFD

information is also shown:

```
DES-7200# show ip rip interface
Serial 0/1 is up, line protocol is up
    Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 packets only
    Receive RIP packet: Enabled
    Send RIP supernet routes: Enabled
    Passive interface: Disabled
    Split horizon: Enabled
    V2 Broadcast: Disabled
    Multicast registe: Registed
    Interface Summary Rip:
      Not Configured
     IP interface address: 2.2.2.111/24
```

Related commands

Command	Description
show ip rip	Show the information of the currently running routing protocol process.

2.2.5 show ip rip peer

Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP peer information.

show ip rip peer [*ip-address*] [**vrf** *vrf-name*]

Parameter description

Parameter	Description
vrf *vrf-name*	Show the RIP interface of specified VRF (optional).
ip-address	Show the specified RIP peer's address (optional).

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

This command is used to show the RIP peer information. If there is no RIP peer, no information will be displayed.

Examples

The following is an example showing the RIP peer information.

```
DES-7200# show ip rip peer
Peer 192.168.3.2:
  Local address: 192.168.3.1
  Input interface: GigabitEthernet 0/2
  Peer version: RIPv1
  Received bad packets: 3
  Received bad routes: 0
     BFD session state up
```

Related commands

Command	Description
show ip rip	Show the information of the currently running routing protocol process.

3 RIPng Commands

3.1 Configuration Related Commands

3.1.1 default-metric(RIPng)

Use this command to define the RIPng default metric value when redistributing other routing protocols. Use the **no** form of this command to restore the default configuration.

default-metric *metric*

no default-metric

Parameter description	**Parameter**	**Description**
	metric	Set the default metric value. The valid range is 1-16. The routing is unreachable if the metric value is larger than or equal to 16.

Default Settings	1
Command mode	Routing process configuration mode.
Usage guidelines	This command shall be co-used with the **redistribute** command. When redistributing the route from one route process to RIPng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPng metric value shall be defined when translating the metric values. If there is no defined metric value, use the **default-metric** command to define one; and the defined metric value will overwrite the value of the **default-metric** command. By default, the **default-metric** value is 1.

Examples

The following example shows how to set the RIPng metric value as 3 when redistributing OSPF process 100:

```
DES-7200(config-router)# default-metric 3
DES-7200(config-router)# redistribute ospf 100
```

Related commands

Command	Description
redistribute	Redistribute the route from one route domain to another route domain.

3.1.2 distance(IPv6)

Use this command to set the RIPng route management distance. Use the **no** form of this command to restore it to the default value.

distance *distance*

no distance

Parameter description

Parameter	Description
distance	Set the RIPng route management distance. The valid range is 1-254.

Default Settings

120.

Command mode

Routing process configuration mode.

Usage guidelines

This command is used to set the RIPng route management distance.

Examples

The following example shows how to set the RIPng route management distance as 160:

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# distance 160
```

3.1.3 distribute-list

Use this command to filter the in/out update route in the prefix-list. Use the **no** form of this command to disable this function.

distribute-list prefix-list *prefix-list-name* {**in** | **out**} [*interface-type interface-name*]

no distribute-list prefix-list *prefix-list-name* {**in** | **out**} [*interface-type interface-name*]

Parameter description

Parameter	Description
prefix-list prefix-list-name	Set the prefix list name and use the prefix list to filter the route.
in | out	Specify to filter the in or out update route in the distribute-list.
interface-type interface-name	(Optional) Apply the distribute-list to the specified interface.

Default Settings

By default, no distribute-list is defined.

Command mode

Routing process configuration mode.

Usage guidelines

This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.

Examples

The following example shows how to filter the received update route on the interface eth0 (only those update routes within the **prefix-list** *allowpre* prefix list range can be received)

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# distribute-list prefix-list allowpre in eth0
```

Related commands

Command	Description
redistribute	Set the route redistribution.

3.1.4 ipv6 rip default-information

Use this command to generate a default IPv6 path to the RIPng. Use the **no** form of this command to delete the default path.

ipv6 rip default-information {**only** | **originate**} [**metric** *metric-value*]

no ipv6 rip default-information

Parameter description

Parameter	Description
only	Advertise the ipv6 default route only.
originate	Not only advertise the ipv6 default route, but also other routes.
metric *metric-value*	Set the metric value for the default route. The valid range is 1-15.

Default Settings

By defaut, no default route is configured.

The default metric value is 1.

Command mode

Interface configuration mode.

Usage guidelines

With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPng route database.

To avoid the route loop, once this command has been configured on the interface, RIPng refuses to receive the default route update message advertised from the neighbor.

Examples

The following example shows how to create a default route to the RIPng routing process on the interface ethernet0/0 and enable this interface to advertise the default route only:

```
DES-7200(config)# interface ethernet 0/0
DES-7200(config-if)# ipv6 rip default-information only
```

Related commands

Command	Description
show ipv6 rip	Show the RIPng process parameters and statistical information.
show ipv6 rip database	Show the RIPng route.

3.1.5 ipv6 rip enable

Use this command to enable the RIPng on the interface. Use the **no** form of this command to disable this function.

ipv6 rip enable

no ipv6 rip enable

Parameter description

Parameter	Description
-	-

Default Settings

N/A

Command mode

Interface configuration mode.

Usage guidelines

This command is used to set the RIPng interface. Before the use of this command, if the RIPng is not enabled, use this command to enable the RIPng automatically.

Examples

The following example shows how to enable the RIPng on the interface 0/0:

```
DES-7200(config)# interface ethernet 0/0
DES-7200(config-if)# ipv6 rip enable
```

3.1.6 ipv6 rip metric-offset

Use this command to set the metric value on the interface. Use the **no** form of this command to cancel the configurations.

ipv6 rip metric-offset *value*

no ipv6 rip metric-offset

Parameter description

Parameter	Description
value	Set the metric value on the interface. The valid range is 1-16.

Default Settings

1

Command mode	Interface configuration mode.
Usage guidelines	Before the route is added to the routing list, the interface metric value shall be upon the route metric. To this end, the interface metric value influences the route usage.

Examples	The following example shows how to set the metric value on the interface ethernet 0/1 as 5:
	`DES-7200(config)# interface ethernet 0/1`
	`DES-7200(config-if)# ipv6 rip metric-offset 5`

3.1.7 ipv6 router rip

Use this command to create the RIPng routing process and enter the routing process configuration mode. Use the **no** form of this command to delete the RIPng routing process.

ipv6 router rip

no ipv6 router rip

Parameter description

Parameter	Description
-	-

Default Settings	No RIPng routing process is running.
Command mode	Global configuration mode.
Usage guidelines	Use this command to create the RIPng routing process and enter the routing process configuration mode.
Examples	The following example shows how to create the RIPng routing process and enter the routing process configuration mode: `DES-7200(config)# ipv6 router rip`

Related commands

Command	Description
ipv6 rip enable	Enable the RIPng on the specified interface.

3.1.8 passive-interface(RIPng)

Use this command to disable the function of the update packet sending on an interface. Use the **no** form of this command to enable this function.

passive-interface {**default** | *interface-type interface-num*}

no passive-interface {**default** | *interface-type interface-num*}

Parameter description

Parameter	Description
default	This parameter sets all interfaces in the passive mode.
interface-type interface-num	Set the interface type and the interface number.

Default Settings

No interface is configured in the passive mode.

Command mode

Routing process configuration mode.

Usage guidelines

The **passive-interface default** command is used to set all interfaces in the passive mode. The **no passive-interface** *intface-type interface-num command* is used to set some interface in the non-passive mode.

Examples

The following example shows how to set all interfaces in the passive mode and set the interface ethernet 0/0 in the non-passive mode:

```
DES-7200(config-router)# passive-interface default
DES-7200(config-router)# no passive-interface ethernet 0/0
```

3.1.9 redistribute

Use this command to redistribute the path in other routing domain to the RIPng. Use the **no** form of this command to cancel the redistribution configurations.

redistribute {**bgp | connected | isis** [*area-tag*] **| ospf** *process-id* **| static**} [**metric** *metric-value* | **route-map** *route-map-name*]

no redistribute {**bgp | connected | isis** [*area-tag*] **| ospf** *process-id* **| static**} [**metric** *metric-value* | **route-map** *route-map-name*]

Parameter description

Parameter	Description
bgp	BGP redistribution.
connected	Connected route redistribution.
isis [*area-tag*]	ISIS redistribution; redistribute the specified ISIS instance using the *area-tag*.
ospf *process-id*	OSPF redistribution; redistribute the specified OSPF instance using the *process-id* with the range of 1-65535..
static	Static route redistribution.
metric *metric-value*	(Optional) set the metric value of path redistributed to the RIPng domain.
route-map *route-map-name*	(Optional) set the redistribution path filtering.

Default Settings

By default, the path of other routing protocols are not redistributed.

If the **default-metric** command is not configured, the default metric value is 1;

By default, the **route-map** is not configured;

By default, all sub-type routes in the specified routing process are redistributed.

Command mode

Routing process configuration mode.

Usage guidelines

This command is used to redistribute the external routing information to the RIPng.

It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different. The RIP and OSPF metric calculations are incomparable for the reason that the RIP metric calculation is hop-based while the

OSPF one is bandwidth-based.

The instance, from where the routing information is redistributed to the RIPng, must be specified in the process of configuring the multi-instance protocol redistribution.

Examples

The following example shows how to redistribute the static route, use the routemap *mymap* to filter and set the metric value as 8:

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# redistribute static route-map mymap metric 8
```

Related commands

Command	Description
default-metric	Define the default RIPng metric value when redistributing other routing protocols.
distribute-list	Distribute and filter the RIPng routing update packets.

3.1.10 split-horizon(RIPng)

Use the **split-horizon** command to enable the RIPng split-horizon function in the routing process configuration mode. Use the **no** form of this command to disable this function. Use the **split-horizon poisoned-reverse** command to enable the RIPng poisoned reverse horizontal split function in the routing process configuration mode. Use the **no** form of this command to disable this function.

split-horizon [**poisoned-reverse**]

no split-horizon [**poisoned-reverse**]

Parameter description

Parameter	Description
poisoned-reverse	(Optional) Enable the poisoned-reverse horizontal split.

Default Settings

Enabled

Command mode

Routing process configuration mode.

Usage guidelines	In the process of packet updating, split-horizon function prevents some routing information from being advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the show ipv6 riip command to determine whether the RIPng split-horizon function is enabled or not.

Examples	The following example shows how to disable the RIPng horizontal split:
	`DES-7200(config)# ipv6 router rip`
	`DES-7200(config-router)# no split-horizon`

3.1.11 timers(ipv6)

Use this command to adjust the RIPng timer. Use the **no** form of this command to restore it to the default value.

timers *update invalid flush*

no timers

Parameter description

Parameter	Description
update	Set the routing update time, in seconds. The *update* parameter defines the period of sending the routing update packets by the device. The *invalid* and *flush* parameter reset once the update packets are received.

invalid	Set the routing invalid time, in seconds, starting from receiving the last valid update packet. The *invalid* parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
flush	Set the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.

Default Settings

The default update time is 30s; the default invalid time is 180s; and the default flush time is 120s.

Command mode

Routing process configuration mode.

Usage guidelines

Adjusting the above time may speed up the RIPng convergence time and the troubleshooting time. The RIPng time must be consistent for the devices connecting to the same network. You are not recommended to adjust the RIP time, except for the specific requirement.

Use the **show ipv6 rip** command to view the current RIPng time parameter setting.

Caution

In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.

Examples

The following example shows how to send the RIP update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds.

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# timers 10 30 90
```

Related commands

Command	Description
show ipv6 rip	Show the parameters and the statistical information of the RIPng process.
show ipv6 rip database	Show the RIPng route.

3.2 Showing Related Commands

3.2.1 show ipv6 rip

Use this command to show the parameters and each statistical information of the RIPng routing protocol process.

show ipv6 rip

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show ipv6 rip
Routing Protocol is "RIPng"
  Sending updates every 10 seconds with +/-50%, next due
```

```
in 8 seconds
  Timeout after 30 seconds, garbage collect after 60
seconds
  Outgoing update filter list for all interface is:
    distribute-list prefix aa out
  Incoming update filter list for all interface is: not
set
  Default redistribution metric is 1
  Default distance is 120
  Redistribution:
     Redistributing protocol connected route-map rm
     Redistributing protocol static
     Redistributing protocol ospf 1
  Default version control:  send version 1, receive
version 1
  Interface              Send   Recv
     VLAN 1             1     1
     Loopback 1          1     1
  Routing Information Sources:
     None
```

Related commands

Command	Description
show ipv6 rip	Show the parameters and each statistical information of the RIPng process.

3.2.2 show ipv6 rip database

Use this command to view the item information in the RIPng routing list.

show ipv6 rip database

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to view the item information in the RIPng routing list.

Examples

```
DES-7200# show ipv6 rip database
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP
sub-codes:n - normal,s - static,d - default,r - redistribute,
          i - interface, a/s - aggregated/suppressed
S(r)   2001:db8:1::/64, metric 1, tag 0
          Loopback 0/::
S(r)   2001:db8:2::/64, metric 1, tag 0
          Loopback 0/::
C(r)   2001:db8:3::/64, metric 1, tag 0
          VLAN 1/::
S(r)   2001:db8:4::/64, metric 1, tag 0
          Null 0/::
C(i)   2001:db8:5::/64, metric 1, tag 0
          Loopback 1/::
S(r)   2001:db8:6::/64, metric 1, tag 0
          Null 0/::
```

Related commands

Command	Description
show ipv6 rip	Show the parameters and each statistical information of the RIPng process.

4 OSPFv2 Commands

4.1 Configuration Related Commands

4.1.1 area

Use this command to configure the specified OSPF area. The **no** form of this command removes the specified OSPF area.

area *area-id*

no area *area-id*

Parameter description

Parameter	Description
area-id	Number of the area where authentication is enabled, a decimal integer or an IP address

Default configuration

No OSPF area is configured by default.

Command mode

Routing process configuration mode.

Usage guidelines

Use the no form of this command to remove the specified OSPF area and its configuration, including the removal of the area-based configuration commands of **area authentication**、**area default-cost**、**area filter-list**、**area nssa**, ect.

Users can not remove the OSPF configuration under the following conditions:

1. It fails to remove all configurations for the backbone area with the virtual link configured. Now the virtual link configuration must be removed before removing the backbone area.
2. The corresponding **network area** command exists in

any area. Now all commands added to the area must be removed before removing this OSPF area.

Examples

The following example removes the configuration of the OSPF area 2:

```
DES-7200(config)# router ospf 2
DES-7200(config-router)# no area 2
```

Related commands

Command	Description
network area	Define the OSPF on the interface and the OSPF area.

4.1.2 area authentication

Use this command to enable authentication in the OSPF area in the routing process configuration mode. The **no** form of this command disables authentication in the OSPF area.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication**

Parameter description

Parameter	Description
area-id	Number of the area where authentication is enabled, a decimal integer or an IP address
message-digest	(optional) MD5 (message digest 5) authentication mode

Default configuration

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

There are three authentication types: 1) 0, no authentication; when this command is not executed to enable OSPF authentication, the authentication type in the OSPF packet is 0; 2) 1, plaintext authentication mode; when this command is configured, the *message-digest* option is not used; 3) 2, MD5 authentication mode; when this command is configured, the *message-digest* option is

used.

All devices in the same OSPF area must have the same authentication type. If the authentication is enabled, authentication password must be configured on the interfaces connecting neighbors. The **ip ospf authentication-key** command in the interface configuration mode can be used to configure the plaintext authentication password. The **ip ospf message-digest-key** command in the interface configuration mode can be used to configure the MD5 authentication password.

Examples

In the following configuration example, MD5 authentication is used in the OSPF routing process area 0 (backbone area), with authentication password "backbone".

```
DES-7200(config)#interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip address
192.168.12.1
255.255.255.0
DES-7200(config-if-FastEthernet 0/1)# ip ospf
message-digest-key 1 md5 backbone
Configure OSPF routing protocol.
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 192.168.12.0
0.0.0.255 area 0
DES-7200(config-router)# area 0 authentication
message-digest
```

Related commands

Command	Description
ip ospf *authentication-key*	Define the OSPF plaintext authentication password.
ip ospf *message-digest-key*	Define the OSPF MD5 authentication password.
area virtual-link	Define a virtual link.

4.1.3 area default-cost

Use this command to define the cost of the default aggregate route that will be advertised to the stub area or NSSA area (OSPF metric) in the routing process configuration mode. The **no** form of this command is used to restore it to the default value.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter description

Parameter	Description
area-id	Number of the stub area or NSSA area
cost	Cost of the default aggregate route that will be advertised to the stub area or NSSA area

Default

The default value is 1.

Command mode

Routing process configuration mode.

Usage guidelines

This command can be configured only on the area border device (ABR) and the ABR must be connected with a stub area or a NSSA area. The so-called ABR means that the device must be connected to at least one area in addition to connecting the backbone area.

There are three commands to configure an OSPF area as a stub or NSSA area : **area stub**, **area nssa** and **area default-cost**. All the devices connecting to the stub area must be configured with the **area stub** command, those connecting to the NSSA area must be configured with the **area nssa** command. However, the **area default-cost** command can be executed only on the ABR.

Examples

Set the cost of the default aggregate route to 50.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.16.0.0 0.0.255.255 area 0
DES-7200(config-router)#network 192.168.12.0 0.0.0.255 area 1
DES-7200(config-router)# area 1 stub
DES-7200(config-router)# area 1 default-cost 50
```

Related commands

Command	Description
area stub	Set an OSPF area as a stub area.
area nssa	Set an OSPF area as a NSSA area.

4.1.4 area filter-list

Use this command to configure the inter-area route filtering on the ABR.

area *area-id* **filter-list** {**access** *acl-name*| **prefix** *prefix-name*} {**in** | **out**}

no area *area-id* **filter-list** {**access** *acl-name* | **prefix** *prefix-name*} {**in** | **out**}

Parameter description

Parameter	Description
area-id	Area ID
acl-name	ACL name
prefix-name	Prefix-list name
access | **prefix**	Associated prefix list or ACL
in | **out**	Apply the ACL rule to the routes incoming/outgoing the area.

Default N/A.

Command mode Routing process configuration mode.

Usage guidelines This command can be configured only on an Area Board Device (ABR) to configure inter area route filtering

Examples Set area 1 to learn only the inter-area routes of 172.22.0.0/8.

```
DES-7200 # configure terminal
DES-7200(config)# access-list 1 permit 172.22.0.0/8
DES-7200(config)# router ospf 100
DES-7200(config-router)# area 1 filter-list access 1 in
```

4.1.5 area nssa

Use this command to set an OSPF area as an NSSA area in the routing process configuration mode. The **no** form of this command is used to delete the NSSA area or the configuration of the NSSA area.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** <*0-16777214*> | **metric-type** <*1-2*>]] [**no-summary**]

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]

Parameter description

Parameter	Description
area-id	NSSA area number

no-redistribution	(Optional) Import the routing information to common areas other than the NSSA area through the **redistribute** command when the device is an ABR of the NSSA area.
default-information originate	(Optional) Generate and import the default type 7 LSA to the NSSA area. This option takes effect only on the NSSA ABR or ASBR.
no-summary	(Optional) Prevent the ABR of the NSSA area from sending types 3 and 4 LSAs into the NSSA area.

Default No NSSA area is defined by default.

Command mode Routing process configuration mode.

Usage guidelines

The parameter **default-information-originate** is used to generate the default Type-7 LSA. This option is slightly different on the NSSA ABR and ASBR. On the NSSA ABR, the default Type-7 LSA will be generated, no matter whether there are default routes in the routing table. On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table.

The parameter **no-redistribution** prevents the OSPF from advertising the external routes imported with the **redistribute** command to the NSSA area on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR.

To further reduce the number of LSAs sent to the NSSA area, you can configure the **no-summary** parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSA) to the NSSA area.

In addition, the **area default-cost** command is used on the ABR of the NSSA area to configure the cost of the default route sent to the NSSA area. By default, the cost of the default route sent to the NSSA area is 1.

Examples Sets area 1 as the stub area on the devices in that area.

```
DES-7200(config)#router ospf 1
```

```
DES-7200(config-router)#network 172.16.0.0 0.0.255.255
area 0
DES-7200 (config-router)#network 192.168.12.0 0.0.0.255
area 1
DES-7200(config-router)# area 1 nssa
```

Related commands

Command	Description
area default-cost	Define the cost (OSPF metric) of the default aggregate route advertised to the NSSA area.

4.1.6 area range

Use this command to configure the route aggregation between OSPF areas in the routing process configuration mode. The **no** form of this command is used to delete the configured route aggregation. The **no** form with the **cost** parameter can restore the default metric of the aggregated route, but not remove route aggregation.

area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area-id* **range** *ip-address net-mask* [**cost** *cost*]

Parameter description

Parameter	Description
area-id	ID of the area the aggreate route is injected into, a decimal integer or an IP address.
ip address	Network segment whose routes are to be aggregated
advertise | not-advertise	Whether to advertise the aggreagate range, advertise by default.
cost *cost*	Set the metric of the aggregated route.

Default

No aggregate route is configured between areas by default.

The default metric of aggregated route depends on whether the device is compatible with RFC1583 or not. If so, the default metric is the smallest cost of the aggregated route. If not, the default metric is the largest cost of the aggregated route.

Command mode

Routing process configuration mode.

Usage guidelines	This command can be executed only on the ABR to aggregate multiple routes of an area to a route and then advertise it to other areas. Route combination occurs only on the border of an area. The devices within an area see the specific routing information, but the devices outside the area only one aggregate route. The advertise and not-advertise options can be used to set whether to advertise the aggregate route, which functions as the filtering and masking purpose. The aggregate route is advertised by default. You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing area. This improves the network forwarding performance, especially in large networks.
Examples	Aggregate the routes of area 1 into a route 172.16.16.0/20. `DES-7200(config)#`**`router ospf`** *`1`* `DES-7200(config-router)#`**`network`** *`172.16.0.0 0.0.15.255`* **`area`** *`0`* `DES-7200((config-router)#`**`network`** *`172.16.17.0 0.0.15.255`* **`area`** *`1`* DES-7200(config-router)#**area** *1* **range** *172.16.16.0 255.255.240.0*

4.1.7 area stub

Use this command to set an OSPF area as a stub area or full stub area in the routing process configuration mode. The **no** form of this command is used to delete the configuration of stub area or full stub area.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter description

Parameter	Description
area-id	STUB area number
no-summary	(Optional) Prevent the ABR from advertising network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.

Default No stub area is defined by default.

Command mode	Routing process configuration mode.
Usage guidelines	All devices in the OSPF stub area must be configured with the **area stub** command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. From the aspect of the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR. The devices in the stub area cannot learn the routes outside the OSPF routing domain. To configure a full stub area, execute **area stub** command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR. There are two commands to configure an OSPF area as a stub area: **area stub** and **area default-cost**. All devices connected to the stub area must be configured with the **area stub** command, but the **area default-cost** command can be executed only on the ABR. The **area default-cost** command defines the initial cost (i.e. metric) of the internal default route.

Examples	Set area 1 as the stub area on the devices in that area.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config-router)# network 172.16.0.0 0.0.255.255 area 0`
	`DES-7200 (config-router)# network 192.168.12.0 0.0.0.255 area 1`
	`DES-7200(config-router)# area 1 stub`

Related commands

Command	Description
area default-cost	Define the cost (OSPF metric value) of the default aggregate route advertised to the stub area.

4.1.8 area virtual-link

To define the OSPF virtual link, execute the **area virtual-link** command in the routing process configuration mode. The **no** form of this command is used to delete the virtual link.

area *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** |**null**]] [**dead-interval** *seconds*] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [[**authentication-key** *key*] | [**message-digest-key** *key-id* **md5** *key*]]

no area *area-id* **virtual-link** *router-id*

Parameter description

Parameter	Description
area-id	OSPF transition area number, a decimal integer or an IP address.
router-id	Identifier of the router neighboring to the virtual link. The router identifier can be viewed through the **show ip ospf** command.
dead-interval *seconds*	(Optional) Define the time to declare neighbor loss (in second), 40 seconds by default. This parameter must be consistent with the neighbor.
hello-interval *seconds*	(Optional)Define the interval at which the HELLO message is sent by the OSPF to the virtual link (in seconds), 10 s by default This parameter must be consistent with the neighbor.
retransmit-interval *seconds*	(Optional) OSPF LSA resend time (in second), 5 seconds by default. The setting of the time must consider the trip time of messages on the link.
transmit-delay *seconds*	(Optional) OSPF LSA send delay (in second), 1 second by default. This value adds the LSA live period. When the LSA live period reaches a certain value, the LSA will be refreshed.
authentication-key *key*	(Optional) Define the OSPF plaintext authentication key. The plaintext authentication key between neighbors must be the same. The **service password-encryption** command enables the key to be displayed in encrypted manner.

message-digest-key *key-id* **md5** *key*	(Optional) Define the OSPF MD5 authentication key identifier and key. The MD5 authentication key identifier and key between neighbors must be the same. The **service password-encryption** command enables the key to be displayed in encrypted manner.
authentication	Set the authentication type to plaintext.
message-digest	Set the authentication type to MD5.
null	Set the authentication type to no authentication

Default

dead-interval: 40s
hello-interval: 10s
retransmit-interval: 5s
transmit-delay: 1s
authentication: no authentication
N/A values for the other parameters

Command mode

Routing process configuration mode

Usage guidelines

In the OSPF routing domain, all areas must be connected with the backbone area. If an area disconnects from the backbone area, it requires to configure virtual links to connect the backbone area. Otherwise, the network communication will become abnormal. The virtual link requires the connection between two ABRs. The area that belongs to both ABRs is called the transition area. A stub Area or NSSA area cannot act as a transition area. Virtual links can also be used to connect other non-backbone areas.

The router-id is the identifier of OSPF neighbor router. If you are unsure of the router-id, check it with the **show ip ospf neighbor** command. You may configure the Loopback address as the router identifier.

The **area virtual-link** command defines only the authentication key for virtual link. To enable the OSPF message authentication for the areas connected with the

virtual link, execute the **area authentication** command in the routing process configuration mode.

Examples

Set area 1 as the transition area to establish virtual link with neighbor 2.2.2.2.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.16.0.0 0.0.15.255 area 0
DES-7200(config-router)# network 172.16.17.0 0.0.15.255 area 1
DES-7200(config-router)# area 1 virtual-link 192.1.1.1
```

Set area 1 as the transition area to establish virtual link with neighbor 1.1.1.1. This virtual link connects area 10 and backbone area, and works with the OSPF message authentication of MD5.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.16.17.0 0.0.15.255 area 1
DES-7200(config-router)# network 172.16.252.0 0.0.0.255 area 10
DES-7200(config-router)# area 0 authentication message-digest
DES-7200(config-router)# area 1 virtual-link 1.1.1.1 message-digest-key 1 md5 hello
```

Related commands

Command	Description
area authentication	Enable the OSPF area message authentication and define the authentication mode.
show ip ospf	Show the OSPF process information, including the router identifier.

4.1.9 auto-cost

Use this command to enable the automatic cost calculating function and set the reference bandwidth. According to the reference bandwidth, you can configure the cost of the specified interface automatically.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter description

Parameter	Description
ref-bw	Reference bandwidth, in the range of 1 to 4294967 Mbps.

Default	100Mbps by default.
Command mode	Routing process configuration mode.
Usage guidelines	This command sets the reference bandwidth for automatically generating interface cost. No parameter with it enables the automatic cost function with a default for the reference bandwidth. A parameter with it enables the automatic cost calculation function with a specified reference bandwidth. Note that the "default auto-cost" and the "no auto-cost" are different: the former restores it to the default and enables the automatic cost function while the latter disables the automatic cost calculation function. If you use **ip ospf cost** command to set the cost of the interface, the cost will replace the auto-cost.

Examples	The configuration example below configures the reference bandwidth as 10M.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config-router)# network 172.16.10.0 0.0.0.255 area 0`
	`DES-7200(config-router)# auto-cost reference-bandwidth 10`

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information

4.1.10 bdf all-interfaces(OSPF)

Use this command to enable the BDF on all OSPF interfaces. The **no** form of this command restores it to the default setting.

bdf all-interfaces

no bdf all-interfaces

Default	Disabled.
Command mode	Routing process configuration mode.

Usage guidelines	The OSPF protocol dynamically discovers the neighbors through the Hello packets. With the BFD function enabled, one BFD session will be established for the neighbors that match the FULL rules and the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPF will perform the network convergence immediately. You can also use the interface configuration mode command **ip ospf bfd** [**disable**] to enable or disable the BFD function on the specified interface, which takes precedence over the command **bfd all-interfaces** in the routing process configuration mode.
Examples	N/A

Related commands

Command	Description
router ospf *process-id* [**vrf** *vrf-name*]	Create the OSPF routing process and enter into the routing process configuration mode.
ip ospf bfd [disable]	Enable or disable the BFD on the specified OSPF interfaces.

4.1.11 clear ip ospf process

Use this command to clear and restart the OSPF instance.

clear ip ospf (*process-id*) **process**

Parameter description

Parameter	Description
process-id	OSPF instance ID When no process ID is specified, the command clears and restarts all the running OSPF instances.

Default	Use the rule recommended in RFC 1583 by default.
Command mode	Privileged mode.
Usage guidelines	

Examples	The command below clears and restarts OSPF instance 1. `DES-7200#clear ip ospf 1 process`

4.1.12 compatible rfc1583

When the routing table includes several routes to the same destination out of the AS, you must determine the best route. Use this command to decide which rule will be taken in RFC 1583 or RFC 2328.

commpatible rfc1583

no commpatible rfc1583

Default	Use the rule recommended in RFC 1583 by default.
Command mode	Routing process configuration mode.

Examples	The configuration example below determines the best route with the rfc 2328 rule.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config-router)# no commpatible rfc1583`

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information

4.1.13 default-information originate (OSPF)

Use this command to generate a default route to the OSPF routing domain in the routing process mode. The **no** form of this command disables the default route.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric** *metric*]

[**metric-type** *type*] [**route-map** *map-name*]

Parameter description

Parameter	Description
Always	(Optional) Generate the default route unconditionally, no matter whether the default route exists locally or not.

metric *metric*	(Optional) Initial metric value of the default route, 1 by default
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different devices; type 2, the same metric seens on different devices. External route of type 1 is more trustworthy than that of type 2. By default, it is type 2.
route-map *map-name*	Associated route map name, no associated route map by default

Default

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

When the **redistribute** or **default-information** command is executed, the OSPF-enabled device automatically turns into the autonomous system border device (ASBR). But the ASBR cannot generate default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR generates default routes by default. It is required to configure with the **default-information originate** routing process configuration command.

If the **always** parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route exists or not. However, the local device does not show the default route. To make sure whether the default route is generated, execute **show ip ospf database** to observe the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. The execution of the **show ip route** command on the OSPF neighbor will display the default route.

The metric of the external default route can be defined only with the **default-information originate** command instead of the **default-metric** command.

There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For

two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the **show ip route** command shows only the type 1 route.

The devices in the stub area cannot generate external default routes.

Examples

The configuration example below generates an external default route to the OSPF routing domain, with type as 1 and metric as 50.

```
DES-7200(config)#router ospf 1
DES-7200(config-router)#network 172.16.24.0 0.0.0.255 area 0
DES-7200(config-router)#default-information originate always metric 50 metric-type 1
```

Related commands

Command	Description
show ip ospf database	Show OSPF link state database.
show ip route	Show the IP routing table.

4.1.14 default-metric

Use this command to configure the default metric of OSPF redistributed route in the routing process mode. The **no** format of this command is used to restore it to the default.

default-metric *metric*

N/A-metric

Parameter description

Parameter	Description
metric	Metric of the OSPF redistributed route

Default The default value is 20.

Command mode Routing process configuration mode.

Usage guidelines

The **default-metric** command must work with the **redistribute** command in the routing process configuration mode to modify the initial metric of all redistributed routes.

The configuration result of the **default-metric** command

	does not take effect for the external routes to the OSPF routing domain via **default-information originate**.

Examples

The configuration example below configures the initial metric of the OSPF redistributed route as 50.

```
Switch(config)# router rip
DES-7200(config-router)# network 192.168.12.0
Switch(config-router)# version 2
DES-7200(config-router)# exit
DES-7200(config)# router  ospf
DES-7200(config-router)# network 172.16.10.0 0.0.0.255
area 0
Switch(config-router)# default-metric 50
DES-7200(config-router)# redistribute rip subnets
```

Related commands

Command	Description
redistribute	Redistribute the routes of other routing processes.
show ip ospf	Show the OSPF global configuration information.

4.1.15 discard-route

Use this command to enable adding the discard route into the kernel routing table. The **no** format of this command is used to disable this function .

discard-route { internal | external }

no discard-route { internal | external }

Parameter description

Parameter	Description
internal	Enable adding the discard route generated by **area range** command
external	Enable adding the discard route generated by the **summary-address** command.

Default Enabled

Command mode Routing process configuration mode.

Usage guidelines After the routing converging, the range may be beyond the actual network range of the routing table. Sending the data

to the nonexistent network within the converging range may cause the routing loop or increase the processing load of the routing device. To prevent it, a discard route is required adding to the routing table on the ABR or the ASBR. This route is generated automatically and will not be transmitted.

Examples

The configuration example below disables adding the discard routes generated by the area range command.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# no discard-route internal
```

Related commands

Command	Description
area range	Configure the route aggregation between OSPF areas
summary-address	Configure the converge route out of the OSPF routing domain

4.1.16 distance ospf

Use this command to set the management distance of different types of routes.

distance {*distance* | **ospf intra-area** *distance* | **inter-area** *distance* | **external** *distance* }

no distance ospf

Parameter description

Parameter	Description
distance	Set the route management distance, 110 default, in the range of 1 to 255.
intra-area *distance*	Set the management distance of the inner-area route, 110 default, in the range of 1 to 255.
inter-area *distance*	Set the management distance of the inter-area route, 110 default, in the range of 1 to 255.
external *distance*	Set the management distance of the external route, 110 default, in the range of 1 to 255.

Default The default value is 110.

Command Routing process configuration mode.

mode	
Usage guidelines	This command is used to specify different management distances for different types of OSPF routes.

Examples	In the configuration below, the OSPF external route management distance is set as 160.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config-router)# distance ospf external 160`

4.1.17 distribute-list in

Use this command to configure LSA filtering.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-type interface-number*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-type interface-number*]

Parameter description

Parameter	Description
access-list-number | *name*	Use the acl filtering rule.
gateway *prefix-list-name*	Use the gateway filtering rule.
prefix *prefix-list-name*	Use the prefix-list filtering rule.
route-map *route-map-name*	Use the route-map filtering rule.
interface-type interface-number	Configure the LSA route filtering on the interface.

Default	N/A.
Command mode	Routing process configuration mode.
Usage guidelines	This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the SPF calculation to generate the corresponding routes. It does not affect the link status database or the routing table of

	the neighbors. It only affects the routing entries calculated by the local OSPF. This function is generally used for the ABR or ASBR, where it can control the routes leaving the area. The following route-map rules will be supported if the route-map parameter is configured: **match interface** **match ip address** **match ip address prefix-list** **match ip next-hop** **match ip next-hop prefix-list** **match metric** **match route-type** **match tag**

Examples	`DES-7200(config)# access-list 3 permit 172.16.0.0 0.0.127.255`
	`DES-7200(config)# router ospf 25`
	`DES-7200(config-router)# redistribute rip metric 100`
	`DES-7200(config-router)# distribute-list 3 in ethernet 0/1`

4.1.18 distribute-list out

Use this command to configure filtering re-distribution routes, similar to the **redistribute** command.

distribute-list {l*istname* | **gateway** *plist-name* | **prefix** *plist-name*} **out** [**bgp** | **connected** | **isis** *area-tag* |**ospf** *process-id* | **rip** | **static**]

no distribute-list {l*istname* | **gateway** *plist-name* | **prefix** *plist-name* } **out** [**bgp** | **connected** | **isis** *area-tag* |**ospf** *process-id*| **rip** | **static**]

Parameter description

Parameter	Description
listname	Use the acl filtering rule.
Gateway *plist-name*	Use the gateway filtering rule.
prefix *plist-name*	Use the prefix-list filtering rule.

	[**bgp** | **connected** | **isis** *area-tag* | **ospf** *process-id* |**rip** | **static**]	Source of the routes to be filtered.

Default	N/A.
Command mode	Routing process configuration mode.
Usage guidelines	The **distribute-list ou**t and the **redistribute route-map** commands are similar. Both filter the routes that other protocols redistribute to the OSPF. However, it does not perform route redistribution by itself. Instead, it works with the **redistribute** command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration.

Examples	The example below filters the redistributed static routes.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config)# redistribute static subnets`
	`DES-7200(config-router)# distribute-list 22 out static`
	`DES-7200(config-router)# distribute-list prefix jjj out static`
	`% There already has filter configured. Please re-configure.`

4.1.19 enable mib-binding

Use this command to bind the MIB with the specified OSPFv2 process. Use the **no** form of this command to restore it to the default value.

enable mib-binding

no enable mib-binding

Parameter description	N/A.
Default	By default, the MIB is binded with the OSPFv2 process in the smallest number.
Command mode	Routing process configuration mode.

Usage guidelines	OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is binded with the OSPFv2 process in the smallest number. The user operations take effect for this process. If the user wants to operate the specified OSPF process by SNMP, use this command to bind the MIB with this process.

Examples	The example below operates the OSPFv2 process 100 by SNMP:
	`DES-7200(config)# router ospf 100`
	`DES-7200(config-router)# enable mib-binding`

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information.
enable traps	Configure the OSPF TRAP function.

4.1.20 enable traps

OSPFv2 process supports 16 kinds of TRAP messages, which are classified into 4 categories. Use this command to enable to send the specified TRAP messages. Use the **no** form of this command to disable to send the specified TRAP messages.

enable traps [**error** [**ifauthfailure | ifconfigerror | ifrxbadpacket | virtifauthfailure | virtifconfigerror | virtifrxbadpacket**] | **lsa** [**lsdbapproachoverflow | lsdboverflow | maxagelsa | originatelsa**] | **retransmit** [**iftxretransmit | virtiftxretransmit**] | **state-change** [**ifstatechange | nbrstatechange | virtifstatechange | virtnbrstatechange**]]

no enable traps [**error** [**ifauthfailure | ifconfigerror | ifrxbadpacket | virtifauthfailure | virtifconfigerror | virtifrxbadpacket**] | **lsa** [**lsdbapproachoverflow | lsdboverflow | maxagelsa | originatelsa**] | **retransmit** [**iftxretransmit | virtiftxretransmit**] | **state-change** [**ifstatechange | nbrstatechange | virtifstatechange | virtnbrstatechange**]]

Parameter description

Parameter	Description
error	Set all traps switches related to the **error**. Use this parameter to set the following specified **error traps** switches:
isa	Set all traps switches related to the **isa**. Use this parameter to set the following specified **isa traps** switches:

error traps	
ifauthfailure	Interface authentication error
ifconfigerror	Interface parameter configuration error
ifrxbadpacket	Error messages are received on the interface
virtifauthfailure	Authentication erroe on the virtual interface
virtifconfigerror	Parameter configuration error on the virtual interface
virtifrxbadpacket	Error messages are received on the virtual interface

isa traps	
lsdbapproachoverflow	External LSA amount has reached the 90% of the upper limit.
lsdboverflow	External LSA amount has reached the upper limit.
maxagelsa	LSA reaches the aging time
originatelsa	Generates new LSA

<table>
<tr><td></td><td>retransmit</td><td>Set all traps switches related to the retransmit. Use this parameter to set the following specified retransmit traps switches:<table><tr><td>iftxretransmit</td><td>Packet retransmission occurs on the interface</td></tr><tr><td>virtiftxretransmit</td><td>Packet retransmission occurs on the virtual interface</td></tr></table></td></tr>
<tr><td></td><td>state-change</td><td>Set all traps switches related to the state-change. Use this parameter to set the following specified state-change switches:<table><tr><td>ifstatechange</td><td>Interface state change</td></tr><tr><td>nbrstatechange</td><td>Neighbor state change</td></tr><tr><td>virtifstatechange</td><td>State change on the virtual interface</td></tr><tr><td>virtnbrstatechange</td><td>State change on the virtual neighbor</td></tr></table></td></tr>
</table>

Default By default, all TRAP switches are disabled.

Command mode Routing process configuration mode.

Usage guidelines The **snmp-server enable traps ospf** command must be configured before configuring this command, for this command is limited by the **snmp-server** command.

This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Examples The example below enables all TRAP switches of the OSPFv2 process 100:

```
DES-7200(config)# router ospf 100
```

```
DES-7200(config-router)# enable traps
```

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information.
enable mib-binding	Bind the OSPFv2 process with MIB.

4.1.21 graceful-restart

Use this command to enable the graceful restart function for the OSPF. The **no** form of the command to restore it to the default setting.

graceful-restart [**graceful-period** *grace-period*]

no graceful-restart [**graceful-period**]

Parameter description

Parameter	Description
grace-period	(optional) Explicitly configure the grace-period.
grace-period	User-set GR interval,in the range of 1 to 1800 seconds, it is the longest time between the OSPF invalidation and the OSPF graceful restart.

Default

By default, the GR function is disabled. And the default value of the grace-period is 120 seconds.

Command mode

Routing process configuration mode.

Usage guidelines

The graceful restart function is configured based on the OSPF instance. According to the actual condition, different instances could be configured with different parameters according to the actual situation.

The graceful restart interval is the longest time between performing the OSPF restart and the graceful restart. In this period, perform the link status reconstruction to restore status of the OSPF to the original. With the interval running out, the OSPF will exit from the GR status and perform the usual OSPF operations.

The GR interval is 120 seconds set by the **graceful-restart** command; the **graceful-restart**

grace-period command allows users changing the interval explicitly.

Examples

The configuration example below enables the GR function for the OSPF instance 1 and sets the restart interval for the GR function.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# graceful-restart
DES-7200(config-router)# graceful-restart grace-period 60
```

Related commands

Command	Description
graceful-restart helper	Enable the OSPF graceful-restart helper.

4.1.22 graceful-restart helper

Use this command to enable the graceful restart helper function. The **no** form of this command restores it to the default setting.

graceful-restart helper {disable | {strict-lsa-checking | internal-lsa-checking}}

no graceful-restart helper {disable | {strict-lsa-checking | internal-lsa-checking}}

Parameter description

Parameter	Description
disable	Disable the graceful restart helper.
strict-lsa-checking	Check the change of the LSA whose types is 1-5,7 to judge the network whether changes. If so, the GR helper will be disabled.
internal-lsa-checking	Check the change of the LSA whose types is 1 -3 to judge the network whether changes. If so, the GR helper will be disabled.

Default

By default, the GR helper is enabled.

With the GR helper enabled, the device dose not check the change of LSA by default.

Command mode

Routing process configuration mode.

Usage guidelines

Use this command to enable the GR helper function. When one neighbor device performs the graceful restart, it sends the Grace-LSA to advertise the all neighbor device. If this device with the GR helper function enabled receives the Grace-LSA, it will become the GR Helper to help the neighbors perform the graceful restart. The **disable** option means that it is not allowed to perform the GR helper function for any device that performs the graceful restart.

After being the GR helper, the device dose not check the network change by default. The convergence is not performed again until the GR is implemented even if the network changes. Use the **strict-lsa-checking** or **internal-lsa-checking** command to enable the fast check for the changed network during the GR. The former checks any LSA (types 1-5,7) that stands for the network information, the latter checks the LSA that stands for the AS inner-area route. In the large scale network, it is not recommended to enable the LSA check option because the local network changes trigger the ending of the GR, resulting in the entire network convergence decreased.

Examples

The configuration example below disables the GF helper and modifies the checking policy of the network changing.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# graceful-restart helper disable
DES-7200(config-router)# no graceful-restart helper disable
DES-7200(config-router)# graceful-restart helper strict-lsa-checking
```

Related commands

Command	Description
gracful-restart	Enable the graceful restart function on the device.

4.1.23 ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of the command to restore it to the default type.

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Parameter description

Parameter	Description
message-digest	Enable MD5 authentication on the interface.
null	Enable no authentication.

Default

No authentication mode is configured on the interface by default. Here, the authentication type of the local area applies on the interface.

Command mode

Interface configuration mode.

Usage guidelines

Plaintext authentication applies when no option is used with the command. Note that the **no** form of this command restores the setting to the default value. Whether authentication is used actually depends on the authentication mode configured for the area of the interface. If the authentication mode is configured as **null**, this enables no authentication. When both the interface and its area are configured with authentication, the one for the interface takes priority.

Examples

The configuration example below configures MD5 authentication for the OSPF on interface fastEthernet 0/1.

```
DES-7200 (config)#interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip address 172.16.1.1
255.255.255.0
DES-7200(config-if-FastEthernet 0/1)# ip ospf authentication
message-digest
```

Related commands

Command	Description
area authentication	Enable authentication and define the authentication mode in the OSPF area.
ip ospf authentication-key	Configure the plaintext authentication key
ip ospf message-digest-key	Configure the MD5 authentication key

4.1.24 ip ospf authentication-key

Use this comand to configure the OSPF plaintext authentication key in the interface configuration mode. The **no** form of this command is used to delete the plaintext authentication key.

ip ospf authentication-key *key*

no ip ospf authentication-key

Parameter description

Parameter	Description
key	Key of at most 8 characters or numerals.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines

The **ip ospf authentication-key** command configures the key that will be inserted in all OSPF message headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key.

To enable the OSPF area authentication, execute the **area authentication** command in the routing process configuration mode.

The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in the interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes priority.

Examples

The configuration example below configures the OSPF authentication key "ospfauth" for the interface fastEthernet 0/0.

```
DES-7200 (config)#interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip address 172.16.1.1
255.255.255.0
```

	`DES-7200(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth`

Related commands

Command	Description
area authentication	Enable authentication in the OSPF area and define the authentication mode
Ip ospf authentication	Enable authentication on the interface and define the authentication mode

4.1.25 ip ospf bdf

Use this command to enable or disable the BFD on the specifed OSPF interface. The **no** form of this command is used to remove the setting on the interface..

ip rip bfd [**disable**]

no ip ospf bfd [disable]

Parameter description

Parameter	Description
disable	Disable the BFD function on the specified OSPF interface.

Default configuration

N/A

Command mode

Interface configuration mode.

Usage guidelines

The command **ip ospf bfd** in the interface configuration mode takes precedence over the **bfd all-interfaces** command in the routing process configuration mode.

You can use this command to enable the BFD on the specified interface according to the actual environment, also can use the command **bfd all-interfaces** in the RIP process configuration mode to enanble the BFD function on all OSPF interfaces and use the command **ip rip bfd disable** to disable the BFD on the specified interface.

Examples

N/A

Related commands

Command	Description
router ospf *process-id* [**vrf** *vrf-name*]	Create the OSPF routing process and enter into the routing process configuration mode.
bdf all-interfaces	Enable the BFD on all OSPF interfaces.

4.1.26 ip ospf cost

Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf cost *cost*

no ip ospf cost

Parameter description

Parameter	Description
Cost	OSPF interface cost

Default

The default cost of the interface is 108/Bandwidth.

Command mode

Interface configuration mode.

Usage guidelines

By default, the OSPF interface cost is 108/Bandwidth, where Bandwidth is the interface bandwidth configured with the **bandwidth** command in the interface configuration mode.

The default costs of different types of lines are as follows:

- 64K serial line: 1562
- E1 line: 48
- 10M Ethernet: 10
- 100M Ethernet: 1

The OSPF cost configured with the **ip ospf cost** command will overwrite the default configuration.

Examples

The configuration example below configures the OSPF cost of the interface fastEthernet 0/1 as 100.

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip ospf cost 100
```

	Command	Description
Related commands	**bandwidth**	Specify the interface bandwidth. This setting does not affect the data transmission rate.
	show ip ospf	Show the OSPF global configuration information

4.1.27 ip ospf database-filter all out

Use this command to configure not to advertise LSA messages on the interface, that is, the LSA update messages are not sent on the interface. The **no** form of the command restores it to the default.

ip ospf database-filter all out

no ip ospf database-filter

Default	This function is disabled by default. Any LSA update message can be sent on the interface.
Command mode	Interface configuration mode.
Usage guidelines	To disable sending LSA update messages on the interface, enable this function on the interface.

Examples	The configuration example below prevents the LSA update messages from being sent on the interface fastEthernet 0/1.
	`DES-7200(config)# interface fastEthernet 0/1`
	`DES-7200(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0`
	`DES-7200(config-if-FastEthernet 0/1)# ip ospf database-filter all out`

4.1.28 ip ospf dead-interval

Use this command to configure the interval to judge the death of interface neighbor in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameter description

Parameter	Description
Seconds	Interval to judge the neighbor death (in seconds)

Default

By default it is 4 times the interval configured with the **ip ospf hello-interval** command.

Command mode

Interface configuration mode.

Usage guidelines

The OSPF death time is included in the Hello message. If the OSPF does not receive the Hello message from its neighbor within the death interval, it declares the neighbor's death and deletes its entry in the neighbor list. By default the death interval is 4 times the interval of the Hello message. The modification of the Hello interval will automatically change the death interval.

This command can be used to manually change the interval to judge the death of OSPF neighbor. Note that:

- The death interval cannot be less than the interval of Hello messages.
- The death intervals of all devices in the same network segment must be the same.

Examples

The configuration example below configures the interval of judging the death of the OSPF neighbor on the interface fastEthernet 0/1 as 30s.

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
DES-7200(config-if-FastEthernet 0/1)# ip ospf dead-interval 30
```

Related commands

Command	Description
ip ospf hello-interval	Specify the interval at which the OSPF sends Hello messages

4.1.29 ip ospf disable all

Use this command to specify the interface not to generate the OSPF messages.

ip ospf disable all

no ip ospf disable all

Default	
Command mode	Interface configuration mode.
Usage guidelines	The interface with this command configured will ignore whether the network area matches or not. After this command is configured, even if the interface belongs to the network, it will not generate OSPF datagram any more. So, it does not receive or send any OSPF message or participate in the OSPF calculation.
Examples	DES-7200(config)# **interface** fastEthernet 0/1 DES-7200(config-if-FastEthernet 0/1)# **ip address** *172.16.10.1 255.255.255.0* DES-7200(config-if-FastEthernet 0/1)# **ip ospf disable all**

4.1.30 ip ospf hello-interval

Use this command to configure the interval to send Hello messages in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter description

Parameter	Description
Seconds	Interval to send Hello messages (in seconds)

Default

- 10s for Ethernet
- 10s for PPP or HDLC encapsulated interfaces
- 10s for frame relay PTP interfaces
- 30s for non-frame relay PTP sub-interface and X.25

	interfaces
Command mode	Interface configuration mode.
Usage guidelines	The interval of sending the Hello messages is included in the Hello message. A shorter interval means OSPF detects the topological change at a faster pace, which will aggravate network traffic. The Hello message intervals for all the devices in the same network segment must be the same. To further manually modify the interval to judge neighbor death, ensure the Hello message interval cannot be greater than the neighbor death interval.

Examples	The configuration example below configures the interval of sending the Hello message on the interface fastEthernet 0/1 as 15.
	`DES-7200(config)# interface fastEthernet 0/1`
	`DES-7200(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0`
	`DES-7200(config-if-FastEthernet 0/1)# ip ospf hello-interval 15`

Related commands

Command	Description
ip ospf dead-interval	Set the interval of judging the death of the OSPF neighbor.

4.1.31 ip ospf message-digest-key

Use this command to configure the MD5 authentication key in the interface configuration mode. The **no** form of this command is used to delete the MD5 authentication key.

ip ospf message-digest-key *key-id* **md5** *key*

no ip ospf message-digest-key

Parameter description

Parameter	Description
Key	Key of up to 16 characters or numerals
key-id	Key identifier in the range of 1 to 255

Default	N/A.

Command mode	Interface configuration mode.
Usage guidelines	The **ip ospf message-digest-key** command configures the key that will be inserted in all OSPF message headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible. The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key. For neighboring devices, the same key identifier must correspond to the same key. To enable authentication in the OSPF area, execute the **area authentication** command in the routing process configuration mode. The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in the interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes priority. The MD5 authentication keys shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF messages by using different keys, till it confirms the neighbors have been configured with new keys. When all devices have been configured with new keys, it is possible to delete the old key.

Examples	The configuration example below adds a new OSPF authentication key "hello5" with key ID 5 for the fastEthernet 0/1.
	`DES-7200(config)# interface fastEthernet 0/1`
	`DES-7200(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0`
	`DES-7200(config-if-FastEthernet 0/1)# ip ospf authentication message-digest`
	`DES-7200(config-if-FastEthernet 0/1)# ip ospf`

```
message-digest-key 10 md5 hello10
DES-7200(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5 md5 hello5
```

When all neighbors are added with new keys, the old keys shall be deleted for all devices.

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# no ip ospf message-digest-key 10 md5 hello10
```

Related commands

Command	Description
area authentication	Enable authentication in the OSPF area and define the authentication mode.
ip ospf authentication	Enable authentication on the interface and define the authentication mode.

4.1.32 ip ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database **description** message. The **no** form of this command is used to restore it to the default.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Default Enabled.

Command mode Interface configuration mode.

Usage guidelines After receiving the database description message, the device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an MTU greater than the interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.

Examples The configuration example below disables the MTU check function on the interface fastEthernet 0/1.

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip ospf mtu-ignore
```

4.1.33 ip ospf network

Use this command to configure the OSPF network type in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf network {broadcast | non-broadcast |

point-to-multipoint [non-broadcast] | point-to-point}

no ip ospf network

Parameter description

Parameter	Description
broadcast	Set the OSPF network type as the broadcast type.
non-broadcast	Set the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
point-to-multipoint [**non-broadcast**]	Set the OSPF network type as the point-to-multipoint type. By default it is the point-to-multipoint broadcast type. The option non-broadcast means point-to-multipoint non-broadcast type.
point-to-point	Set the OSPF network type as the point-to-point type.

Default

- PTP network type: PPP, SLIP, frame relay PTP sub-interface, X.25 PTP sub-interface encapsulation
- NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface)
- Broadcast network type: Ethernet encapsulation
- By default, the network type is the point-to-multipoint network type.

Command mode

Interface configuration mode.

Usage guidelines

Networks are divided into three types according to the transmission feature of media:

- Broadcast network (Ethernet, token ring and FDDI)

- Non-broadcast network (frame relay and X.25)
- PTP network (HDLC, PPP and SLIP)

The non-broadcast network is further divided into two sub-types by the OSPF operation mode:

- Non-broadcast multi-path access (NBMA) type. NBMA requires all interconnected devices can directly communicate to each other, and only full mesh type connection can meet this requirement. There is no problem in case of the SVC (such as X.25) connections, but it is difficult in case of networking with PVC (such as frame relay). The OSPF on the NBMA network operates similarly to that on the broadcast network, where the Designated Device shall be elected to advertise the link state of the NBMA network.
- The second is the point-to-multipoint network type. If the network topology is not a mesh type non-broadcast network, the OSPF requires the network type to be configured as the point-to-multipoint network type. In the point-to-multipoint network type, the OSPF regards all inter-device connections as PTP links and do not participate in the election of the designated device. The point-to-multipoint network type is further divided into broadcast type and non-broadcast type. For the non-broadcast type, it is required to manually configure the static neighbor.

Whatever the default network type of the interface, you must set it to the broadcast network type. For example, the non-broadcast multi-path access network (frame relay and X.25) can be configured as broadcast network, so that the configuration of neighbors can be omitted during the OSPF routing process configuration. The **X.25 map** and **frame-relay map** commands may enable the X.25 and frame relay networks with broadcasting capability, so that the OSPF can regard such networks as X.25 and frame relay as broadcast network.

The interface of the point-to-multipoint network can be configured with one or more neighbors. When the OSPF is configured as the point-to-multipoint network type, multiple host routes may be generated. In contrast to the broadcast network type, the point-to-multipoint network type features the following benefits:

- Easy configuration without configuration of neighbors or election of designated device
- Small cost, without needing the fully meshed topology

For the dial-up network, frame relay and X.25 network, to manually configure the IP address mapping table, the keyword "broadcast" must be specified to support broadcast.

Examples

The configuration example below configures the frame relay interface network as the broadcast type, which is applicable for the full mesh type frame relay connections.

```
DES-7200(config)# interface Serial1/0
DES-7200(config-if-Serial 1/0)# ip address 172.16.24.4
255.255.255.0
DES-7200(config-if-Serial 1/0)# encapsulation
frame-relay
DES-7200(config-if-Serial 1/0)# ip ospf network broadcast
```

The configuration example below configures the frame relay interface network as the point-to-multipoint type, which is applicable for the non-full-mesh type frame relay connections.

```
DES-7200(config)# interface Serial1/0
DES-7200(config-if-Serial 1/0)# ip address 172.16.24.4
255.255.255.0
DES-7200(config-if-Serial 1/0)# encapsulation
frame-relay
DES-7200(config-if-Serial 1/0)# ip ospf network
point-to-multipoint
```

The configuration example below configures the frame relay interface network as the broadcast type, with DR/RDR specified, which is applicable for the full or partial mesh type frame relay connections. The configuration below needs to be done on all branch node devices and non-designated devices (limited to become DR/BDR).

```
DES-7200(config)# interface Serial1/0
DES-7200(config-if-Serial 1/0)# ip address 172.16.24.4
255.255.255.0
DES-7200(config-if-Serial 1/0)# encapsulation
frame-relay
DES-7200(config-if-Serial 1/0)# ip ospf network broadcast
DES-7200(config-if-Serial 1/0)# ip ospf priority 0
```

Related commands

Command	Description
dialer map ip	Define the map between IP address and dialing number.

frame-relay map	Define the map between IP address and frame DLCI.
neighbor (OSPF)	Define the IP address of neighbor applicable for NBMA network type and point-to-multipoint non-broadcast type only.
X25 map	Define the map between IP address and X.25 network address.

4.1.34 ip ospf priority

Use this command to configure the priority in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf priority *priority*

no ip ospf priority

Parameter description

Parameter	Description
Priority	Set the priority of the interface.

Default

The default priority is 1.

Command mode

Interface configuration mode.

Usage guidelines

The interface priority is included in the Hello message. When DR/BDR (designated device/backup designated device) election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid for only OSPF broadcast and non-broadcast network types.

Note: If the DR and BDR exist in the network, the modification of the interface priority will not take effect immediately. The new priority will not be used until the next DR and BDR election occurs.

Examples

The configuration example below configures the priority of the interface fastethernet 0/1 as 0.

```
Switch(config)#interface fastethernet 0/1
```

```
DES-7200(config-if-FastEthernet 0/1)# ip ospf priority 0
```

Related commands

Command	Description
ip ospf network	Configure the network type of the interface.

4.1.35 ip ospf retransmit-interval

Use this command to define the interval to send the link state update message on the interface in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter description

Parameter	Description
seconds	Interval to send the link state update message. This interval must be greater than the trip delay of packets between two neighbors. The default is 5 seconds.

Default The default is 5 seconds.

Command mode Interface configuration mode.

Usage guidelines

When the device sends an LSU message completely, the LSU message stays in the send buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the **ip ospf retransmit-interval** command, the LSA will be sent once again.

In serial lines or virtual links, the resend interval shall be slightly larger. The LSU message resend interval of virtual link is defined through the **area virtual-link** command followed with the keyword **retransmit-interval**.

Examples

The configuration example below configures the LSU message resend interval on the interface fastEthernet 0/1 as 10 seconds.

```
DES-7200(config)# interface fastEthernet 0/1
```

	`DES-7200(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10`

Related commands	**Command**	**Description**
	area virtual-link	Define an OSPF virtual link.

4.1.36 ip ospf transmit-delay

Use this command to define the LSU message transmission delay in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter description	**Parameter**	**Description**
	Seconds	LSU message transmission delay (in seconds). The default is 1 second.

Default	The default is 1 second.
Command mode	Interface configuration mode.
Usage guidelines	Before the LSU message is transmitted, the Age field in all the LSAs of the message will be increased by the value defined in the interface configuration command **ip ospf transmit-delay**. The configuration of this parameter shall consider the send and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU message transmission delay of virtual link is defined through the **area virtual-link** command followed with the keyword retransmit-interval. the LSA is resent or requested resending with Age up to 3600. If no refresh is obtained in time, the aged LSA will be cleared from the link state database.
Examples	The configuration example below configures the transmission delay of fastEthernet 0/1 as 5.

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10
```

Related commands

Command	Description
area virtual-link	Define an OSPF virtual link.

4.1.37 log-adj-changes

Use this command to enable the logging of the neighbor state changes. The **no** or **default** form of the command is used to disable it.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter description

Parameter	Description
Seconds	LSU message transmission delay (in seconds). The default is 1 second.

Parameter description

Parameter	Description
detail	Record the detail of changes.

Default

Enabled. Without the **detail** parameter, the system records the logs that the neighbor enters the full state or leaves the full state.

Command mode

Routing process configuration mode.

Examples

The configuration example below logs the neighbor status change.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# log-adj-changes
```

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information.

4.1.38 max-concurrent-dd

Use this command to specify the maximum number of DD messages that can be processed (initiate or accept) at the same time.

max-concurrent-dd *<1-65535>*

Parameter description

Parameter	Description
<1-65535>	Maximum number of DD messages

Default The default value is 5.

Command mode Interface configuration mode.

Usage guidelines When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD messages that each OSPF instance can have at the same time.

Examples In the configuration example below, the maximum number of DD messages is set as 4.

```
DES-7200(config)# router ospf 10
DES-7200(config-router)# max-concurrent-dd 4
```

4.1.39 max-metric

Use this command to set the maximum metric of the router-lsa, so that this routing device will not firstly be used as the transmission node by other devices in SPF computing. The **no** form of this command is used to cancel the maximum metric.

max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** [*seconds*]] [**summary-lsa** [*max-metric-value*]]

no max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** [*seconds*]] [**summary-lsa** [*max-metric-value*]]

Parameter description

Parameter	Description
router-lsa	Set the maximum metric (0XFFFF) of non-stub links in the Router LSA.
external-lsa	Use the maximum metric instead of the external-lsa metric. (including the Type-5 and Type-7)

max-metric-value	Maximum metric value of the LAS, 16711680 by default, in the range of 1 to 16777215.
include-stub	Set the maximum metric of the stub links in the Router LSA.
on-startup	Advertise the maximum metric when the routing device starts up.
seconds	Interval of advertising the maximum metric, 600s by default, within the range of 5 to 86400.
summary-lsa	Use the maximum metric instead of the summary LSA metric. (including the Type-3 and Type-4)

Default Normal metric LSAs.

Command mode Routing process configuration mode.

Usage guidelines

With the command **max-metric router-lsa** enabled, maximum metric of non-stub links in the Router LSA generated by the routing device is set. The link's normal metric is restored after canceling this configuration or reaching the timer.

By default, with this command enabled, the normal metric of the stub links is still advertised, which is the output interface cost. If the **include-stub** parameter is configured, the maximum metric of the stub links will be advertised.

When the device acts as an ABR, if no interval flow transmission is expected, use the **summary-lsa** parameter to set the summary LSA as the maximum metric.

When the device acts as an ASBR device, if no external flow transmission is expected, use the **external lsa** parameter to set the external LSA as the maximum metric.

the **max-metric router-lsa** command is usually used in the following scenes:

- Restart the device, which generally makes the IGP protocol converged faster, so that other devices attempt forwarding the dataflow through the new started-up device. If current device remains establishing a BGP routing table, the packets sent to these networks will be discarded due to some BGP routings have not been

learned. In this case, use the **on-startup** parameter to set certain delay, so that this device can be servers as a transmission node after restarting.

- The device is added into the network without being used for dataflow transmission. If the backup path exists, the current device is not used for the dataflow transmission. Otherwise, this device is still used to transmit the dataflow.
- Remove the device from the network gracefully. With this command enabled, the current device advertises the maximum metric to all devices, as that the other devices in this network can choose the backup path to for the dataflow transmission before it closes.

Note

For the OSPF implementation in the old version (RFC 1247 or earlier versions), the links with maximum metric in the LSA will not anticipate the SPF calculation, that is, no dataflow will be sent to these LSAs router.

Examples

The configuration example below sets to advertise the maximum metric as 100 seconds after starting the device.

```
DES-7200(config)# router ospf 20
DES-7200(config-router)# max-metric router-lsa on-startup 100
```

Related commands

Command	Description
show ip ospf	Show the ospf related configurations.

4.1.40 neighbor

Use this command to define the OSPF neighbor in the routing process configuration mode. The **no** form of this command is sued to delete the specified neighbor.

neighbor *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost]*

no neighbor *ip-address*

Parameter description

Parameter	Description
ip address	IP address of the neighbor

	poll-interval *seconds*	(Optional) Specify the interval of polling neighbors (in seconds), 120 s by default. Only the non-broadcast (NBMA) network type supports this option.
	priority *priority*	(Optional) Configure the priority of non-broadcast network neighbors, 0 by default. Only the non-broadcast (NBMA) network type supports this option.
	Cost *cost*	(Optional) Configure the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. Only the point-to-multipoint [non-broadcast] network type supports this option.

Default	N/A.
Command mode	Routing process configuration mode.

Usage guidelines

You must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface.

In the NBMA network, if the neighbor device becomes inactive, in other words, the Hello message is not received within the device death interval, the OSPF will send more Hello messages to the neighbor. The interval at which the Hello messages are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello messages only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello messages to all neighbors to establish the neighbor relationship.

Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the "cost" option for the point-to-multipoint network type.

Examples

The configuration example below declares an OSPF non-broadcast network neighbor, with IP address 172.16.24.2, priority 1 and polling interval 150s.

```
DES-7200(config)# router ospf 20
DES-7200(config-router)# network 172.16.24.0 0.0.0.255 area 0
DES-7200(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related commands

Command	Description
ip ospf priority	Set the interface priority.
ip ospf network	Set the network type

4.1.41 network area

Use this command to define which interfaces run OSPF and the OSPF areas they belong to in the routing process configuration mode. The **no** form of this command is used to delete the OSPF area definition of the interface.

network *ip-address wildcard* **area** *area-id*

no network *ip-address wildcard* **area** *area-id*

Parameter description

Parameter	Description
ip addres	IP address of the interface
wildcard	Define the comparison bits in the IP address, 0 for exact match and 1 for no comparison
area-id	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as the OSPF area identifier.

Default

There is no OSPF area configured by default.

Command mode

Routing process configuration mode.

Usage guidelines

The parameters *ip-address* and *wildcard* allow associating multiple interfaces with one OSPF area. To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by **network area**. Only secondary IP address is not enough to enable OSPF on the interface.

If the IP address of the interface matches the IP address ranges defined by the **network** command in multiple OSPF processes, you can determine the OSPF process that the interface takes part in by the means of best match.

Examples

The configuration example below defines three areas: 0, 1 and 172.16.16.0. Define the interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1, define the interfaces whose IP addresses fall into the 172.16.16.0/20 range to area 2, and define the remaining interface to area 0.

```
DES-7200(config)# router ospf 20
DES-7200(config-router)# network 172.16.16.0
0.0.15.255 area 172.16.16.0
DES-7200(config-router)# network 192.168.12.0
0.0.0.255 area 1
DES-7200(config-router)# network 0.0.0.0
255.255.255.255 area 0
```

Related commands

Command	Description
router ospf	Create OSPF routing process

4.1.42 overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance.

overflow database <*1-4294967294*> **[hard | soft]**

no overflow database

Parameter description

Parameter	Description
<*1-4294967294*>	Maximum number of LSAs
hard | **soft**	hard: Shut down the OSPF instance when the number of LSAs exceeds that number. soft: Issue an alarm when the number of LSAs exceeds that number.

Command mode

Routing process configuration mode.

Usage guidelines

To shut down the OSPF instance when the number of LSAs exceeds that number, use the "hard" parameter; otherwise, use the "soft" parameter.

Examples

In the configuration below, when there are more than 10 LSAs, OSPF instance 10 will be shut down.

```
DES-7200# config terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# overflow database 10 hard
```

4.1.43 overflow database external

Use this command to configure the maximum number of external LSAs and the waiting time from overflow status to normal status.

overflow database external *max-dbsize wait-time*

no overflow database external

Parameter description

Parameter	Description
max-dbsize	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS)
wait-time	Waiting time of the routing device from the overflow status to normal status.

Default

By default the *max-dbsize* is -1 and the *wait-time* is 0 second.

Command mode

Global configuration mode.

Examples

In the configuration below, the maximum number of external LSAs is configured as 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow status to the normal status is 3 seconds.

```
DES-7200# config terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# overflow database external 10 3
```

4.1.44 overflow memory-lack

Use this command to allow the OSPF to enter the OVERFLOW state when the memory lacks. Use the **no** form of this command to disabe this function.

overflow memory-lack

no overflow memory-lack

Parameter description

Parameter	Description
no	Disable the function of entering the OVERFLOW state when the memory lacks.

Default

By default, OSPF is allowed to enter the OVERFLOW state when the memory lacks..

Command mode

Routing process configuration mode.

Usage

The action of OSPF entering the OVERFLOW state is to

guidelines	discard the newly-learned external route and prevent the memory from being increased effectively. It is possible that enabling this function causes the route loop in the whole network. To reduce that occurance possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state. Use the **clear ip ospf process** command to reset the OSPF and remove the OSPF OVERFLOW state. Use the **no** form of this command to disallow the OSPF to enter the OVERFLOW state when the memory lacks, which may result in the constantly consume of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.

Examples	The configuration example below disallows the OSPF to enter the OVERFLOW state when the memory lacks.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config-router)# no overflow memory-lack`

Related commands

Command	Description
clear ip ospf process	Reset the OSPF instances.
show ip protocols ospf	Show the OSPF information.

4.1.45 passive-interface

Use this command to configure the specified network interface or all interface as the passive interfaces. The **no** format of this command is used to restore it to the default.

passive-interface {**default** | *interface-type interface-number*}

no passive-interface {**default** | *interface-type interface-number*}

Parameter description

Parameter	Description
interface-type interface-number	The interface to be set as a passive one.
default	Set all the interfaces as passive interfaces.

Default	By default, no interface is configured as passive interface. All interfaces are allowed to receive/send OSPF messages.
Command mode	Routing process configuration mode.
Usage guidelines	To prevent other devices in the network from dynamically learning the routing information of the device, specify the specified network interface of this device as passive interface.

Examples	The configuration example below configures fastEthernet 0/1 as passive interface.
	`DES-7200(config)# router ospf 30`
	`DES-7200(config-router)# passive-interface fastEthernet 0/1`

Related commands

Command	Description
show ip ospf interface	Show the configuration information of the interface.

4.1.46 redistribute

Use this command to redistribute the external routing information.

redistribute {**bgp** | **ospf** *process-id* | **rip** | **connected** | **static**}[**metric** *value* | **match** {**internal** | **external** | **external 1** | **external 2** | **nssa-external** | **nssa-external 1** | **nssa-external 2**}**metric-type** {*1*|*2*} | **route-map** *map-tag* | **tag** <*0-4294967295*> | **subnets**]

no redistribute {**bgp** | **ospf** *process-id* | **rip** | **connected** | **static**}[**metric** *value* | **match** {**internal** | **external** | **external 1** | **external 2** | **nssa-external** | **nssa-external 1** | **nssa-external 2**}**metric-type** {*1*|*2*} | **route-map** *map-tag* | **tag** <*0-4294967295*> | **subnets**]

Parameter description

Parameter	Description
bgp | **ospf** *process-id*| **rip** | **connected** | **static**	Redistribute the routes of the specified routing protocol.
metric	Set the metric of OSPF extern2 LSA.

match	Redistribute the specific OSPF routes. By default, all the OSPF routes are redistributed.
metric-type	Set the external routing type as E-1 or E-2.
route-map	Redistribution filter rule.
tag	Set the tag value of the routes redistributed to the OSPF.
subnets	Redistribute the routes of non standard networks.

Default N/A

Command mode Route configuration mode.

Usage guidelines

After the command is configured, the routing device will turn to ASBR, the related routing information is imported into the OSPF domain and broadcasted to other OSPF routing device through type-5 LSAs.

For redistribution, the default metric of BGP routes is 1; the default metric of the LSAs generated by other types of routes is 20.

When you configure redistributing OSPF routes without the **match** parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The **no** form of this command restores the setting to the default value.

When you filter routes for redistribution by following the **route-map** rule, the **match** rule of the **route-map** rule is specific for the original redistribution parameters. It is only when the redistributed OSPF routes follow the **match** rule that the **route-map** rule works.

Examples

The following command redistributes static routes to the OSPF domain.

```
DES-7200(config-router)# redistribute static subnets
DES-7200(config)# router ospf 1
DES-7200(config-router)# redistribute ospf 2 subnets
```

```
DES-7200(config-router)# redistribute ospf 2 match external 1 internal
```

The following is the results of the **show run** command.

```
router ospf 1
redistribute ospf 2 match external 1 internal subnets
```

4.1.47 router ospf

Use this command to create the OSPF routing process in the global configuration mode. The **no** form of this command is used to delete the defined OSPF routing process.

router ospf *process-id* [**vrf** *vrf-name*]

no router ospf [*process-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID
vrf-name	VRF name

Default N/A.

Command mode Global configuration mode.

Usage guidelines Different OSPF instances are mutually independent and can be approximately considered as two routing protocols without mutual interference.

Examples The following example creates the OSPF routing process 10 within the specified vrf: *vpn_1*

```
DES-7200(config)# router ospf 10 vrf: vpn_1
```

Related commands

Command	Description
show ip protocols	Show the routing protocol informatin.
show ip ospf	Show the OSPF information.

4.1.48 router ospf max-concurrent-dd

Use this command to specify the maximum number of DD messages that can be processed (initiate or accept) at the same time.

router ospf max-concurrent-dd *number*

no router ospf max-concurrent-dd

Parameter description

Parameter	Description
number	Maximum number of DD messages, in the range of 1 to 65535.

Default The default value is 10.

Command mode Interface configuration mode.

Usage guidelines When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD messages that each OSPF instance can have (initiate or accecpt) at the same time.

Examples In the configuration example below, the maximum number of DD messages is set as 4.

```
DES-7200(config)# router ospf 10
DES-7200(config-router)# router ospf max-concurrent-dd 4
```

Related commands

Command	Description
max-concurrent-dd	Set the maximum number of the neighbor concurrent with the OSPF routing process

4.1.49 router-id

Use this command to set the router ID. Use the **no** form of this command to delete the setting or restore it to the default.

router-id *router-id*

no router-id

Parameter description

Parameter	Description
router-id	Router ID in IP address form

Default configuration By default, the OSPF routing process will select the maximal interface IP address as the router ID.

Command mode	Routing process configuration mode.
Usage guidelines	You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a large number of works. It is not recommended to change the router ID. The device can be changed only when no LSA is generated. To configure the OSPF protocol, you should execute this command to specify the ID of a device. Certainly, you can also specify it by the loopback. At this time, you should configure the router ID before configuring the OSPF protocol.

Examples	The following example modifies the router ID to 0.0.0.36
	`DES-7200(config)# router ospf 20`
	`DES-7200(config-router)# router-id 0.0.0.36`

Related commands

Command	Description
show ip protocols	Show the routing protocol information.

4.1.50 summary-address

Use this command to configure the converge route out of the OSPF routing domain in the routing process configuration mode. The **no** form of this command is used to delete the converged route.

summary-address *ip-address net-mask* [**not-advertise | tag** *<0-4294967295>* |]

no summary-address

Parameter description

Parameter	Description
ip address	IP address of the converged route
net-mask	Network mask of the converged route
not-advertise	Do not advertise the converged route.

Default	No converged route is configured by default.

Command mode	Routing process configuration mode.
Usage guidelines	When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous border device can advertise only one converged route, reducing the scale of routing table greatly. Unlike the **area rang** command, the former involves the convergence of routes between OSPF areas, while the latter involves the convergence of external routes of the OSPF routing domain. For the NSSA area, the **summary-address** command is valid only on the ABR of the NSSA now, and causes the convergence for only redistributed routes.

Examples	The configuration command below generates an external converged route 100.100.0.0/16.
	`DES-7200(config)# router ospf 20`
	`DES-7200(config-router)# summary-address 100.100.0.0 255.255.0.0`
	`DES-7200(config-router)# redistribute static subnets`
	`DES-7200(config-router)# network 200.2.2.0 0.0.0.255 area 1`
	`DES-7200(config-router)# network 172.16.24.0 0.0.0.255 area 0`
	`DES-7200(config-router)# area 1 nssa`

Related commands

Command	Description
area-range	Configure route convergence on the OSPF area border device.

4.1.51 timers lsa arrival

Use this command to configure the time delay for the same LSA recieved. The **no** form of the command restores it to the default.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter description

Parameter	Description
arrival-time	Configure the time delay when receiving the same LSA, in the range of 0 to 600000.

Default 1000 milliseconds.

Command mode Routing process configuration mode.

Usage guidelines When the same LSA is received within the specified time, no action will be done.

Examples

The configuration example below configures the time delay for the same LSA as 2s.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# timers arrival-time 2000
```

Related commands

Command	Description
show ip ospf	Show the OSPF information.

4.1.52 timers pacing lsa-group

Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for aged link state. The **no** form of the command restores it to the default.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter description

Parameter	Description
seconds	This parameter is used for LSA pacing, checksum calculation, and aging interval. The range is 10 to1800s.

Default 240 seconds.

Command mode	Routing process configuration mode.
Usage guidelines	The updated information in the pacing switch (LSA), checksum calculation, and aging interval are for more efficient switch use. The default is 4 minutes. This parameter needs not to be adjusted often. The optimum group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better. To configure OSPF LSA pacing, follow these steps in the privileged mode:

Examples	The configuration example below configures the pacing time as 120s.
	`DES-7200(config)# device ospf 20`
	`DES-7200 (config-router)# timers paing lsa-group 120`

Related commands

Command	Description
show ip ospf	Show the OSPF information.

4.1.53 timers pacing lsa-transmit

Use this command to transmit the LSA grouping updating. The **no** form of the command restores it to the default.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter description

Parameter	Description
transmit-time	Set the interval of sending the LSA grouping, in the range of 10 to 1000.
transmit-count	Set the number of LS-UPD packets per group, in the range of 1 to 200.

Default	Transmit-time: 40 milliseconds. Transmit-count: 10

Command mode	Routing process configuration mode.
Usage guidelines	In the environment that there are a large number of LSAs and the load on the system is too much, you can properly use the **transmit-time** and **transmit-count** to inhibit the flooding LS-UPD packets number in the network. While the CPU and network bandwidth loads are not too much, reduce the transimi-time and increase the transimit-count to quicken the environment convergence.

Examples	The configuration example below sets the interval of sending the LS-UPD packets as 50ms, the packets number as 20.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config-router)# timers pacing lsa-transmit 50 20`

Related commands

Command	Description
show ip ospf	Show the OSPF information.

4.1.54 timers spf

Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations in the routing process configuration mode. The **no** form of this command restores it to the default.

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter description

Parameter	Description
spf-delay	Define the SPF calculation waiting period, in seconds. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation. Range: 0-2147483647.

	spf-holdtime	Define the interval between two SPF calculations, in seconds. When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start. Range: 0-2147483647.

Default	The default values are: spf-delay: 5s; spf-holdtime: 10s. By default, the **timers spf** command takes no effect. Spf-delay depends on the default configuration of the **timers throttle spf** command.
Command mode	Routing process configuration mode.
Usage guidelines	Shorter values *of spf-delay* and *spf-holdtime* mean OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the device. **Note:** The configurations of the **timers spf** command and the **timers throttle spf** command are overwritten.

Examples	The configuration example below configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.
	`DES-7200(config)# device ospf 20`
	`DES-7200(config-router)# timers spf 3 9`

Related commands	**Command**	**Description**
	show ip ospf	Show the configuration information of the ospf.

4.1.55 timers throttle lsa all

Use this command to configure the exponential backoff algorithmin for the LSA in the routing process configuration mode. The **no** form of this command restores it to the default.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter description

Parameter	Description
delay-time	Configure the time delay of generating the LSA first, in the range of 1 to 600000.
hold-time	Set the minimum interval of refreshing the LSA between the first time and second time, in the range of 1 to 600000.
max-wait-time	Set the maximum interval of successive refreshing the LSA in the range of 1 to 600000, which determines whether the LSA is refreshed successively.

Default

Delay-time: 0 millisecond,
Hold-time: 5000 milliseconds,
Max-wait-time: 5000 milliseconds.

Command mode

Routing process configuration mode.

Usage guidelines

If the high convergence perfermance for the link change is demanded, the delay-time can be relatively small. if you expect to reduce the CPU consumption, increase appropriately sevel values.

Caution

The hold-time cannot be smaller than the delay-time, and the max-wait-time cannot smaller thant he hold-time.

Examples

The configuration example below configures the first delay as 10ms, hold-time as 1s and the longest delay as 5s.

```
DES-7200(config)# router ospf 1

DES-7200(config-router)# timers throttle lsa all 10 1000 5000
```

Related commands

Command	Description
show ip ospf	Show the configuration information of the ospf

4.1.56 timers throttle spf

Use this command to configure the topology change information for OSPF, including the delay for SPF calculation as well as the interval between two SPF calculations in the routing process configuration mode. The **no** form of this command restores it to the default.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter description

Parameter	Description
spf-delay	Define the SPF calculation waiting period, in milli-seconds. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Define the interval between two SPF calculations, in seconds. When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.
spf-max-waittime	Define the maximum interval between two SPF calculations, in milli-seconds, with the valid range from 1 to 600000.

Default

spf-delay: 1000ms; spf-holdtime: 5000ms; spf-max-waittime: 10000ms.

Command mode

Routing process configuration mode.

Usage guidelines

Spf-delay refers to the delay time of the topology change to the SPF calculation. *Spf-holdtime* refers to the minimum interval between two SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval till it reaches to *spf-max-waittime*. If the interval between two SPF calculations has exceeded the required value, the SPF calculation will re-start from *spf-holdtime*.

Smaller *spf-delay* and *spf-holdtime* value can make the topology faster. Greater *spf-max-waittime* value can reduce the SPF calculation. Those configurations can be flexible according to the actual stability of the network

topology.

Compared with the **timers spf** command, this command is more flexible. It not only speeds up the SPF calculation convergence, but also reduces the system resources consumption of SPF calculation due to the topology change. To this end, the **timers throttle spf** command is recommended.

Note:

1. The spf-holdtime cannot be smaller than spf-delay, or the spf-holdtime will be set to be equal to spf-delay;
2. The spf-max-waitime cannot be smaller than spf-holdtime, or the spf-max-waittime will be set to be equal to spf-holdtime automatically;
3. The configurations of the **timers spf** command and the **timers throttle spf** command are overwritten.
4. Without neither **timers spf** command and **timers throttle spf** command configured, the default value is the one of the timers throttle spf command.

Examples

The configuration example below configures the delay and holdtime and the maximum time interval of the OSPF as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculations are: 5ms，1s，3s，7s，15s，31s，63s，89s，179s，179+90 ……

```
DES-7200(config)# router ospf 20
DES-7200(config-router)# timers spf 5 1000 90000
```

Related commands

Command	Description
show ip ospf	Show the configuration information of the ospf

4.1.57 two-way-maintain

Use this command to enable the OSPF two-way-maintain function. The **no** form of this command disables this function.

two-way-maintain

no two-way-maintain

Parameter description

Parameter	Description
-	-

Default Enabled.

Command mode Routing process configuration mode.

Usage guidelines

In the large-scale network, partial packets delay or dropped may exist due to much CPU and memory are occupied caused by large numbers of packets transmission. If the Hello packets are handled over the dead interval, the corresponding adjacency will disconnected. In this case, enable the two-way-maintain function for the packets such as DD, LSU, LSR and LSAck packets from certain neighbor in the network (except for the Hello packets), avoiding the neighbor invalidation caused by the Hello packets delay or dropped.

Examples

The configuration example below disables the OSPF two-way-maintain function.

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# no two-way-maintain
```

Related commands

Command	Description
show ip ospf	Show the configuration information of the ospf

4.2 Showing Related Commands

4.2.1 show ip ospf

Use this command to show the OSPF information in the privileged user mode.

show ip ospf [*process-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	This command shows the information of the OSPF routing process.

Examples	The output results of the **show ip ospf** command are as follows:
	`DES-7200# show ip ospf`
	`Routing Process "ospf 1" with ID 1.1.1.1`
	`Process uptime is 4 minutes`
	`Process bound to VRF default`
	`Conforms to RFC2328, and RFC1583Compatibility flag isenabled`
	`Supports only single TOS(TOS0) routes`
	`Supports opaque LSA`
	`This device is an ASBR (injecting external routing information)`
	`SPF schedule delay 5 secs, Hold time between two SPFs 10 secs`
	`LsaGroupPacing: 240 secs`
	`Number of incomming current DD exchange neighbors 0/5`
	`Number of outgoing current DD exchange neighbors 0/5`
	`Number of external LSA 4. Checksum 0x0278E0`
	`Number of opaque AS LSA 0. Checksum 0x000000`
	`Number of non-default external LSA 4`
	`External LSA database is unlimited.`
	`Number of LSA originated 6`
	`Number of LSA received 2`
	`Log Neighbor Adjency Changes : Enabled`
	`Number of areas attached to this device: 1`
	`  Area 0 (BACKBONE)`
	`Number of interfaces in this area is 1(1)`
	`Number of fully adjacent neighbors in this area is 1`
	`Area has no authentication`
	`SPF algorithm last executed 00:01:26.640 ago`
	`SPF algorithm executed 4 times`
	`Number of LSA 3. Checksum 0x0204bf`
	`  Area 1 (NSSA)`
	`Number of interfaces in this area is 1(1)`
	`Number of fully adjacent neighbors in this area is 0`
	`Number of fully adjacent virtual neighbors through this area is 0`

```
Area has no authentication
SPF algorithm last executed 02:09:23.040 ago
SPF algorithm executed 4 times
Number of LSA 6. Checksum 0x028638
NSSA Translator State iselected
```

The fields in the displayed results are described as follows:

Field	Description
Router id	Router id
Process uptime	Effective time of the current OSPF process (the process does not take effect when the device-id is 0.0.0.0)
Bound to VRF	The VRF of the current OSPF
Conforms to RFC2328	The same as the RFC2328
RFC1583Compatibility flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external route. This policy is used in the selection of best ASBR and in the route comparison.
Support Tos	Only TOS0 is supported.
Supports opaque LSA	Supporting opaque-LSA
Device Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	This parameter is used for LSA pacing, checksum calculation, and aging interval.
Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status

	for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.
Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this device	Total number of areas on the devices
Area type	`Area type`, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent	Number of Full neighbors

neighbors in this area	of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSA Translator State	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA area.

4.2.2 show ip ospf border-routers

Use this command to show the OSPF internal routing table on the ABR/ASBR in the privileged user mode.

show ip ospf [*process-id*] **border-mrouters**

Parameter description

Parameter	Description
process-id	OSPF process ID

Command mode

Privileged user mode.

Usage guidelines

This command shows the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the **show ip route** command. The OSPF internal

routing table has destination address of the router id instead of destination network.

Examples

The output results of the **show ip ospf border-mrouters** command are as follows:

```
DES-7200# show ip ospf border-devices
OSPF internal Routing Table

Codes: i - Intra-area route, I - Inter-area route
```

i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select

The fields in the displayed results are described as follows:

Field	Description
Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.
I	Intra-area routes
1.1.1.1	Show the OSPF ID of the border device.
[2]	Show the cost to the border device.
via 10.0.0.1	Show the next-hop gateway to the border device.
FastEthernet 0/1	Show the interface to the border device.
ABR, ASBR	Show the type of the border device, including ABR, ASBR, or both
Area 0.0.0.1	Show the area that learns the route
select	When there are multiple paths to the ASBR, the select indicates the currently selected optimal path.

4.2.3 show ip ospf database

Use this command to show the OSPF link state database information in the privileged user mode.

Different formats of the command will display different LSA information.

show ip ospf [*process-id area-id*] **database**

show ip ospf [*process-id area-id*] **database** [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**self-originate** | **max-age**]

show ip ospf [*process-id area-id*] **database** [**device**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**device**] [**adv-device**

ip address

show ip ospf [*process-id area-id*] **database** [**device**] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**network**][*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**]

[*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**]

[*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**]

[*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**external**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**external**] [*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**external**] [*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**nssa-external**]

[*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**nssa-external**]

[*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*]**database** [**nssa-external**] [*link-state-id*] [**self-originate** | **maxage**]

show ip ospf [*process-id area-id*]**database** [**database-summary**]

Parameter description

Parameter	Description
area-id	(Optional) Area ID displayed
adv-device	(Optional) Show the LSA information generated by the specified advertising device.
link-state-id	(Optional) Show the LSA information of the specified OSPF link state identifier.
self-originate	(Optional) Show the LSA information generated by the device itself.
maxage	(Optional) Display the LSAs aged.
device	(Optional) Show the OSPF device LSA information.
network	(Optional) Show the OSPF network LSA information.
summary	(Optional) Show the OSPF summary LSA information.
asbr-summary	(Optional) Show the ASBR summary LSA information.
external	(Optional) Show the OSPF external LSA information.
nssa-external	(Optional) Show the category 7 OSPF external LSA information.
opaque-area	(Optional) Show type 10 LSAs.
opaque-as	(Optional) Show type 11 LSAs.
opaque-link	(Optional) Show type 9 LSAs.
database-summary	(Optional) Show the statistics of LSAs of the link state database.

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	When the OSPF link state database is very large, you should show the information on the link state database in many ways. Proper use of these commands may help OSPF troubleshooting.
Examples	The output results of the **show ip ospf database** command are as follows:

```
DES-7200# show ip ospf database
OSPF Device with ID (1.1.1.1) (Process ID 1)
Device Link States (Area 0.0.0.0)
Link ID        ADV Device     Age  Seq#      CkSum  Link
count
1.1.1.1        1.1.1.1        2    0x80000011 0x6f39 2
3.3.3.3        3.3.3.3        120  0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID        ADV Device     Age  Seq#      CkSum
192.88.88.27    1.1.1.1        120  0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID        ADV Device     Age  Seq#      CkSum
Route
10.0.0.0       1.1.1.1        2    0x80000003 0x350d
10.0.0.0/24
100.0.0.0      1.1.1.1        2    0x8000000c 0x1ecb
100.0.0.0/16
Device Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Device     Age  Seq#      CkSum  Link
count
1.1.1.1        1.1.1.1        2    0x80000001 0x91a2 1
        Summary Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Device     Age  Seq#      CkSum
Route
100.0.0.0      1.1.1.1        2    0x80000001 0x52a4
100.0.0.0/16
192.88.88.0     1.1.1.1        2    0x80000001 0xbb2d
192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Device     Age  Seq#      CkSum
Route            Tag
20.0.0.0       1.1.1.1        1    0x80000001 0x033c E2
20.0.0.0/24     0
100.0.0.0      1.1.1.1        1    0x80000001 0x9469 E2
100.0.0.0/28    0
```

```
AS External Link States
Link ID         ADV Device      Age  Seq#       CkSum
Route            Tag
20.0.0.0        1.1.1.1         380  0x8000000a 0x7627 E2
20.0.0.0/24     0
100.0.0.0       1.1.1.1         620  0x8000000a 0x0854 E2
100.0.0.0/28    0
```

The fields in the displayed results of the **show ip ospf database** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Device Link States	Show the device LSA information.
Net Link States	Show the network LSA information.
Summary Net Link States	Show the summary network LSA information.
NSSA-external Link States	Show the type 7 autonomous external LSA information.
AS External Link States	Show the type 5 autonomous external LSA information.
Link ID	Link ID
ADV Device	ID of the device that advertises the LSAs
Age	Show the live period of the LSA.
Seq#	Show the sequentce number of the LSA, which is used to check aged or duplicate LSA.
Cksum	Show the checksum of the LSAs.
Link-Count	Show the number of links in the device LSA information.
Route	Show the device information included in the LSA.
Tag	Show the tag of the LSA

The output results of the **show ip ospf database asbr-summary** command are as follows:

```
DES-7200# show ip ospf database asbr-summary
     OSPF Device with ID (1.1.1.35) (Process ID 1)
```

```
        ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Device address)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
     TOS: 0  Metric: 1
```

The fields in the displayed results of the **show ip ospf database asbr-summary** command are described as follows:

Field	Description
OSPF Device with ID	Router id
AS Summary Link States	Show the summary LSA information in the AS.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.

The output results of the **show ip ospf database external** command are as follows:

```
DES-7200# show ip ospf database external
     OSPF Device with ID (1.1.1.35) (Process ID 1)
```

```
        AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

The fields in the displayed results of the **show ip ospf database external** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Type-5 AS External Link States	Show autonomous external LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
Metric Type	Indicate the external link type.
TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.

Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The output results of the **show ip ospf database network** command are as follows:

```
DES-7200# show ip ospf database network
     OSPF Device with ID (1.1.1.1) (Process ID 1)

         Network Link States (Area 0.0.0.0)
LS age: 572
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.88.88.27 (address of Designated
Device)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x5366
Length: 32
Network Mask: /24
     Attached Device: 1.1.1.1
     Attached Device: 3.3.3.3
```

The fields in the displayed results of the **show ip ospf database network** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Network Link States	Show the network LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.

Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the network corresponding to the LSA.
Attached Device	Show the device that is connected with the network.

The output results of the **show ip ospf database device** command are as follows:

```
DES-7200# show ip ospf database device
     OSPF Device with ID (1.1.1.1) (Process ID 1)
        Device Link States (Area 0.0.0.0)
LS age: 322
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: device-LSA
Link State ID: 1.1.1.1
Advertising Device: 1.1.1.1
LS Seq Number: 80000012
Checksum: 0x6d3a
Length: 48
Number of Links: 2

Link connected to: Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metric: 0
```

The fields in the displayed results of the **show ip ospf database device** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Device Link States	Show the device LSA information.

LS age	Show the live period of the LSA.
Options	Option
Flag	Flag
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Number of Links	Show the number of links associated with the device.
Link connected to	Show what the link is connected to and the network type.
(Link ID)	Link identifier
(Link Data)	Link data
Number of TOS metrics	TOS value; support TOS0 only
TOS 0 Metrics	TOS0 metric

The output results of the **show ip ospf database summary** command are as follows:

```
DES-7200# show ip ospf database summary
     OSPF Device with ID (1.1.1.1) (Process ID 1)
        Summary Link States (Area 0.0.0.0)
LS age: 499
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
     TOS: 0  Metric: 11
```

The fields in the displayed results of the **show ip ospf database summary** command are described as follows:

Field	Description

OSPF Device with ID	Router id
Summary Net Link States	Show the summary network LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.

The output results of the **show ip ospf database nssa-external** command are as follows:

```
DES-7200# show ip ospf database nssa-external
     OSPF Device with ID (1.1.1.1) (Process ID 1)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 1
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x033c
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     NSSA: Forward Address: 100.0.2.1
     External Route Tag: 0
```

The fields in the displayed results of the **show ip ospf database nssa-external** command are described as follows:

Field	Description
OSPF Device with ID	Router id
NSSA-external Link States	Show the type 7 autonomous external LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequential number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
Metric Type	Show the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.
NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The output results of the **show ip ospf database external** command are as follows:

```
RDES-7200# show ip ospf database external
     OSPF Device with ID (1.1.1.1) (Process ID 1)
        AS External Link States
```

```
LS age: 1290
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

The fields in the displayed results of the **show ip ospf database external** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Type-7 AS External Link States	Show the type 7 autonomous external LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
Metric Type	Show the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.

Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

Following is the display result of show ip ospf database database-summary command:

```
DES-7200# show ip ospf database database-summary
OSPF process 1:
Device Link States      : 4
Network Link States     : 2
Summary Link States     : 4
ASBR-Summary Link States : 0
AS External Link States  : 4
NSSA-external Link States: 2
```

The description of the fields displayed with the command **show ip ospf database database-summary** is as below:

Field	Description
OSPF Process	OSPF process ID
Device Link	Number of device LSAs in the area
Network Link	Number of network LSAs in the area
Summary Link	Number of summary LSAs in the area
ASBR-Summary Link	Number of ASBR summary LSAs in the area
AS External Link	Number of NSSA LSAs in the area
NSSA-external Link	Number of NSSA LSAs in the area

4.2.4 show ip ospf interface

Use this command to show the OSPF-associated interface information in the privileged user mode.

show ip ospf interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	(Optional) type of the specified interface
interface-number	(Optional) number of the specified interface

Default N/A.

Command mode Privileged mode.

Usage guidelines This command shows the OSPF information on the interface.

Examples

The output results of the **show ip ospf interface fastEthernet** *0/1* command are as follows:

```
DES-7200# show ip ospf interface fastEthernet 0/1
FastEthernet 0/1 is up, line protocol is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500
Matching network config: 192.88.88.0/24
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
Designated Router (ID) 1.1.1.1, Interface Address 192.88.88.27
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 70784
Hello received 1786 sent 1787, DD received 13 sent 8
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

The fields in the displayed results of the **show ip ospf interface serial** *1/0* command are described as follows:

Field	Description
FastEthernet 0/1 State	State of the network interface; UP means normal working and Down means faults.
Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router id	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay
State	DR/BDR state ID
Priority	Priority of the interface
Designated Device(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router id of the BRD of the interface
BDR's Interface address	Address of the BDR of the interface
Time intervals configured	The Hello, Dead, Wait, and Retransmit intervals of the interface
Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of **Full** neighbors
Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received

DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received
Discard	Statistics on the discarded OSPF packets

4.2.5 show ip ospf neighbor

Use this command to show the OSPF neighbor list in the privileged user mode.

show ip ospf [*process-id*] **neighbor** [[**detail**] | [[*interface-type interface-number*] [*neighbor-id*]]]

Parameter description

Parameter	Description
Detail	(Optional) Show the neighbor details.
interface-type interface-number	(Optional) Show the neighbor information of the specified interface
neighbor-id	(Optional) Show the information of the specified neighbor

Default N/A.

Command mode Privileged mode.

Usage guidelines This command shows neighbor information usually used to check whether the OSPF is running normally.

Examples The output results of the **show ip ospf neighbor** command are as follows:

```
DES-7200# show ip ospf neighbor
Neighbor 3.3.3.3, interface address 192.88.88.72
In the area 0.0.0.0 via interface FastEthernet 0/1
Neighbor priority is 1, State is Full, 11 state changes
```

```
DR is 192.88.88.27, BDR is 192.88.88.72
Options is 0x52 (*|O|-|EA|-|-|E|-)
Dead timer due in 00:00:32
Neighbor is up for 05:11:27
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Crypt Sequence Number is 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timer on
Graceful-restart helper disabled
BFD session state up
```

The fields in the displayed results of the **show ip ospf neighbor** command are described as follows:

Field	Description
Neighbor ID	Neighbor ID
Pri	Neighbor priority (for selection of DR)
State	Neighbor status
Dead Time	Remaining time for the neighbor to enter the Dead status
Address	The corresponding interface address of the neighbor
Interface	The corresponding interface of the neighbor
interface address	The interface address of the neighbor device
In the area	Show the area that learns the neighbor.
via interface	Show the interface that learns the neighbor
Neighbor priority	Priority of the neighbor OSPF

State	OSPF neighbor connection state. FULL means the stable state; DR indicates that the neighbor is the designated device; BDR indicates that the neighbor is the backup designated device; DROTHER indicates that the neighbor is not a DR/BDR. Point-to-point network type has no DR or DBR.
State changes times	Times of state changes
Dead Time	Dead time of the neighbor
DR	Interface address of the DR elected of the neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected of the neighbor device (that is, the BDR field of the Hello packet)
Options	Hello packet E-bit option, where 0 indicates that the area is a STUB area; 2 indicates that the area is not a STUB area.
Dead timer due in	Dead time of the neighbor device
Neighbor up time	Period from when the device is discovered till now
Database Summary List	Statistics on the neighbor DD packets
Link State Request List	Statistics on the neighbor LS request packets
Link State Retransmission List	Statistics on the neighbor re-transmit packets
Crypt Sequence Number	Area MD5 authentication code
Thread Inactivity Timer	Status of invalid neighbor timer

Thread Database Description Retransmission	Status of DD packet timer of the interface
Thread Link State Request Retransmission	Status of LS request packet timer of the interface
Thread Link State Update Retransmission	Status of LS update packet timer of the interface
Thread Poll Timer	Poll Timer start status of the static neighbor

4.2.6 show ip ospf route

Use this command to show the OSPF routes.

show ip ospf [*process-id*] **route** [**count**]

Parameter description

Parameter	Description
process-id	OSPF process ID. All OSPF routes will be shown without an ID specified.
Count	Show the statistics of various OSPF routes.

Command mode

Privileged mode.

Examples

```
DES-7200# show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF,
IA - OSPF inter area  N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 0/1
C  192.88.88.0/24 [1] is directly connected,FastEthernet
0/1,Area 0.0.0.1
```

The description of every field shown via command show ip ospf routeis as below:

Field	Description
codes	Route type and correspond abbreviation and description

100.0.0.0/24	Route prefix
[1]	Route cost
via	Route next hop and interface

4.2.7 show ip ospf spf

Use this command to show the routing count in the OSPF area.

show ip ospf [*process-id*] **spf**

Parameter description

Parameter	Description
process-id	OSPF process ID.

Command mode

Privileged User mode.

Usage guidelines

This command is used to show the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.

Examples

```
DES-7200# show ip ospf 1 spf

OSPF process 1:

Area_id     30min_counts   Total_counts

0               32             1235

1               6               356
```

The description of every field shown via command **show ip ospf** [*process-id*] **spf** as below:

Field	Description
Area_id	OSPF area ID.
30min_counts	The OSPF routing counts within the latest 30 minutes.
Total_counts	Total counts of the OSPF routing till now.

Related commands

Command	Description
show ip ospf	Show the OSPF summary.

4.2.8 show ip ospf summary-address

Use this command to show the converged route of all redistributed routes in the privileged user mode.

show ip ospf summary-address

Command mode	Privileged mode.
Usage guidelines	This command is valid only on the NSSA ABR, and shows only the routes with local convergence operation.

Examples

The output results of the **show ip ospf summary-address** command are as follows:

```
DES-7200#show ip ospf summary-address
Summary Address Summary Mask  Advertise  Status
Aggregated subnets
------------ ------------ ------------ --------
--------------
202.101.0.0    255.255.0.0    advertise    Inactive 0
DES-7200#
```

Parameter	Description
Summary Address	IP address to be converged
Summary Mask	Mask to be converged
Advertise	Whether to advertise the converged route
Status	The convergence range takes effect or not
Aggregated subnets	Number of external routes included in the converged route

4.2.9 show ip ospf virtual-link

Use this command to show the OSPF virtual link information in the privileged user mode.

show ip ospf [*process-id*] **virtual-link**

Command mode	Privileged mode.

Usage guidelines

If no virtual link is configured, the command only shows the neighbor status as well as other related information. The **show ip ospf neighbor** command does not show the neighbor of virtual link.

Examples

The output results of the **show ip ospf virtual-links** command are as follows:

```
DES-7200# show ip ospf virtual-links
Virtual Link VLINK0 to device 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 0/1
Local address 10.0.0.37/32
Remote address 10.0.0.27/32
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 00:00:05
Adjacency state Full
```

The fields in the displayed results are described as follows:

Field	Description
Virtual Link VLINK0 to device	Show the virtual link neighbors and their status.
Virtual Link State	Show the virtual link state.
Transit area	Show the transit area of the virtual link.
via interface	Show the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Show the transmit delay of the virtual link.
State	Interface state
Time intervals configured	The Hello, Dead, Wait, and Retransmit interval of the interface
Adjacency State	Neighbor state, where FULL means the stable state

5 OSPFv3 Commands

5.1 Configuration Related Commands

5.1.1 area default-cost

Use this command to set the cost of the default route for the ABR in the stub area. Use the **no** form of this command to restore it to the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter description

Parameter	Description
area-id	Area ID of the stub area. It can be an integer or an IPv4 prefix.
cost	Cost of the default route of the stub area in the range 1 to 16777214.

Default configuration

By default, the cost of the default route is 1.

Command mode

OSPFv3 configuration mode.

Usage guidelines

This command can only work in the ABR connected to the stub area.

Examples

The following example sets the cost of the default route of stub area 50 to 100.

```
ipv6 router ospf 1
area 50 stub
area 50 default-cost 100
```

Related commands

Command	Description
area stub	Set a stub area.

	show ipv6 ospf area	Show the OSPFv3 area information.

5.1.2 area-range

Use this command to set the range of the converged inter-area addresses. Use the **no** form of this command to remove the setting or restore it to the default setting.

area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise|not-advertise**]

no area *area-id* **range** *ipv6-prefix*/*prefix-length*

Parameter description

Parameter	Description
area-id	ID of the area in which the addresses are converged. It can be an integer or an IPv4 prefix.
ipv6-prefix/prefix-length	Range of the converged addresses.
not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.

Default configuration

No converged inter-area address range is defined.

Command mode

OSPFv3 configuration mode.

Usage guidelines

This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. In this way, the number of the routes in the OSPF AS is reduced.

Use **no area** *area-id* to delete the area including all the configuration of the area.

Examples

The following example converges the routes in area 1.

```
ipv6 router ospf 1
area 1 range 2001:abcd:1:2::/64
```

Related

Command	Description

	discard-route	Add the discard route generated by the OSPF process to the core routing table.
	summary-prefix	Set the range of the external routes to be converged.

5.1.3 area stub

Use this command to create a stub area or set its attributes. Use the **no** form of this command to restore the stub area to an ordinary area or delete its configuration.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

	Parameter	Description
Parameter description	*area-id*	ID of the stub. It can be an integer or an IPv6 prefix.
	no-summary	This option applies only to the ABR in the stub area, indicating that the ABR only advertises the type 3 LSA indicating the default route to the stub area, not other type 3 LSAs.

Default configuration	None.
Command mode	OSPFv3 configuration mode.
Usage guidelines	Use **no area** *area-id* **stub** command to restore the area as a common area. Use **no area** *area-id* to delete the area including all the configuration of the area. By default, the ABR in the stub area only generates and then advertises the type 3 LSA indicating the default route to the stub area. While the ABR in the NSSA area generates and then advertises the type 3 LSA indicating the default route to the NSSA area only after **no-summary** is used.
Examples	The following example enables the ABR in stub area 10 to

advertise the default route to the stub area.

```
ipv6 router ospf 1
area 10 stub
area 10 stub no-summary
```

Related commands

Command	Description
area default-cost	Set the cost of the default route in the stub area.
show ipv6 ospf area	Show the OSPFv3 area information.

5.1.4 area virtual-link

Use this command to create a virtual link or set its parameters. Use the **no** form of this command to delete the virtual link or restore it to the default setting.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*]

no area *area-id* **virtual-link** *router-id* [**hello-interval**] [**dead-interval**][**retransmit-interval**] [**transmit-delay**] [**instance**]

Parameter description

Parameter	Description
area-id	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
Router-id	Neighbor router ID of the virtual link.
hello-interval *seconds*	Set the interval to send the hello message on the local virtual link interface in the range from 1 to 65535s. The default value is 10s.
dead-interval *seconds*	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. Its range is 1 to 65535s, and the default value is four times the value of **hello-interval**.
retransmit-interval *seconds*	Specify the interval for the local interface of the virtual link to retransmit LSA. The range is from 1 to 65535s, and the default value is 5s.
transmit-delay	Specify the delay for the local

seconds	interface of the virtual link to wait before sending LSA. The range is from 1 to 65535s, the default value is 1s.
instnace *instance-id*	Specify the instance corresponding to the virtual like.

Default configuration

No virtual link is defined.

Command mode

OSPFv3 configuration mode.

Usage guidelines

In the OSPF AS, all the areas must be connected with the backbone area to ensure that they can learn the routes of the whole OSPF AS. If an area cannot be directly connected with the backbone area, it can connect it through a virtual link.

Note:

- The virtual link shall not be in the stub or NSSA area.
- **hello-interval**, **dead-interval** and **instance** shall be configured consistently on both sides of the virtual link, otherwise neighboring relationship cannot be set up between the virtual neighbors.
- Use **no area** *area-id* to delete the area including all the configuration of the area.

Examples

The following example configures a virtual link.

```
ipv6 router ospf 1
area 1 virtual-link 192.1.1.1
```

Related commands

Command	Description
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.
show ipv6 ospf virtual-links	Show the OSPFv3 virtual link information.

5.1.5 auto-cost

The metric of the OSPF protocol is the interface-based bandwidth. Use this command to enable the bandwidth-based interface metric calculation or modify the reference bandwidth. Use the **no** form of this command to disable the bandwidth-based interface metric calculation or restore it to the default reference bandwidth.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter description

Parameter	Description
reference-bandwidth *ref-bw*	Specify the reference bandwidth In the range 1 to 4294967 Mbps. The default value is 100Mbps.

Default configuration

The interface metric is calculated based on the reference bandwidth, which is 100Mbps.

Command mode

OSPFv3 configuration mode.

Usage guidelines

Use **no auto-cost reference-bandwidth** to restore it to the default reference bandwidth.

You can use **ipv6 ospf cost** in the interface configuration mode to set the cost of the specified interface, and it takes precedence over the metric calculated based on the reference bandwidth.

Examples

The following example changes the reference bandwidth to 10M.

```
ipv6 router ospf 1
auto-cost reference-bandwidth 5
```

Related commands

Command	Description
ipv6 ospf cost	Set the cost of the interface.
show ipv6 ospf	Show the OSPFv3 routing process information.

5.1.6 bdf all-interfaces(OSPFv3)

Use this command to enable the BDF on all OSPFv3 interfaces. The **no** form of this command restores it to the default setting.

bdf all-interfaces

no bdf all-interfaces

Default	Disabled.
Command mode	Routing process configuration mode.
Usage guidelines	The OSPFv3 protocol dynamically discovers the neighbors through the Hello packets. With the BFD function enabled, one BFD session will be established for the neighbors that match the FULL rules and the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPFv3 will perform the network convergence immediately. You can also use the interface configuration mode command **ipv6 ospf bfd** [**disable**] to enable or disable the BFD function on the specified interface, which takes precedence over the command **bfd all-interfaces** in the routing process configuration mode.
Examples	N/A

Related commands

Command	Description
ipv6 router ospf *process-id*	Create the OSPFv3 routing process and enter into the routing process configuration mode.
ipv6 ospf bfd [disable]	Enable or disable the BFD on the specified OSPFv3 interfaces.

5.1.7 clear ipv6 ospf process

Use this command to clear and restart the OSPF process.

clear ipv6 ospf {**process** | *process-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID ranging from 1 to 65535

Command mode	Privileged mode.
Usage guidelines	In normal case, it is not necessary to use this command.

Examples	The example below restarts the OSPF process.
	`en`
	`clear ipv6 ospf process`

5.1.8 default-information originate

Use this command to generate a default route to the OSPF routing domain in the routing process mode. The **no** form of this command disables the default route.

default-information originate [always] [metric *metric***] [metric-type** *type***] [route-map** *map-name***]**

no default-information originate [always] [metric] [metric-type] [route-map *map-name***]**

Parameter settings

Parameter	Description
always	(Optional) Generate the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric value of the default route, with the valid range of 0 to 16777214, 1 by default
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric sees on different routers. External route of type 1 is more trustworthy than that of type 2. By default, it is type 2.
route-map *map-name*	Associated route-map name, no associated route-map by default

Default	None

Command mode	Routing process configuration mode
Usage guideline	When the **redistribute** or **default-information** command is executed, the OSPF-enabled router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate default route automatically or advertise it to all the routers in the OSPF routing domain. The ASBR generates default routes by default. It is required to configure with the **default-information originate** routing process configuration command. If the **always** parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route exists or not. However, the local router does not show the default route. To make sure whether the default route is generated, execute **show ipv6 ospf database** to observe the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. The execution of the **show ipv6 route** command on the OSPF neighbor will display the default route. The metric of the external default route can be defined only with the **default-information originate** command instead of the **default-metric** command. There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the **show ipv6 route** command shows only the type 1 route. The routers in the stub area cannot generate external default routes.
Examples	The configuration example below generates a default route. `default-information originate always`

Related commands

Command	Description
redistribute	Redistribute routes.

	show ipv6 ospf	Show the OSPFv3 route information.
	show ipv6 ospf database	Show OSPFv3 link state database

5.1.9 default-metric

Use this command to set the default metric for the routes to be redistributed. Use the **no** form of this command to restore it to the default setting.

default-metric *metric-value*

no default-metric

Parameter description	**Parameter**	**Description**
	metric-value	Default metric for the routes to be redistributed. Its range is 1 to 16777214, and the default value is 20.

Default configuration	20.
Command mode	OSPFv3 configuration mode.
Usage guidelines	This command can be used with **redistribute** together to set the default metric for the routes to be redistributed. But this command does not appliy to two types of routes: 1. The default route generated with **default-information originate**; 2. The redistributed direct route, which always uses 20 as the default metric value.
Examples	The following example sets the default metric for the routes to be redistributed to 10. `default-metric 10`

Related	**Command**	**Description**

redistribute	Redistribute the routes.
show ipv6 ospf	Show the OSPFv3 routing process information.

5.1.10 distance

Use this command to set the management distance of different types of OSPFv3 routes. The **no** form of this command restores it to the defualt setting.

distance {*distance* **| ospf { intra-area** *distance* **| inter-area** *distance* **| external** *distance* **}}**

no distance [ospf]

Parameter description

Parameter	Description
intra-area *distance*	Set the management distance of the inner-area route, in the range of 1 to 255.
inter-area *distance*	Set the management distance of the inter-area route, in the range of 1 to 255.
external *distance*	Set the management distance of the external route, in the range of 1 to 255.
distance	Set the management distance of the route, in the range of 1 to 255.

Default

The default value is 110.

Management distance of the inner-area route :110,

Management distance of the inter-area route :110

Management distance of the external-area route :110

Command mode

Routing process configuration mode.

Usage guidelines

This command is used to specify different management distances for different types of OSPF routes. The management distance of the route is used for the comparison of routing priority, the smaller the management distance is, the higher the routing priority.

The priority of the route generated by different OSPFv3 processes must be compared using the management distance.

Setting the management distance as 255 indicates the

routing entry is untrusted and it will not join the packet forwarding.

Examples

In the configuration below, the OSPFv3 external route management distance is set as 160.

```
DES-7200(config)# ipv6 router ospf 20
DES-7200(config-router)# distance ospf external 160
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process .

5.1.11 ipv6 ospf area

Use this command to enable the interface to participate in the OSPFv3 routing process. Use the **no** form of this command to disable this function.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID.
area *area-id*	OSPFv3 area in which the interface participates in. It can be an integer or an IPv6 prefix.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to enable the interface to participate in the OSPFv3 routing process. If **ipv6 router ospf** is not used to start the OSPFv3 routing process, it will be automatically started after this command is used.

Use **no ipv6 ospf area** to disable the specified interface from participating in the OSPFv3 routing process.

Use **no ipv6 router ospf** to disable all the interfaces from

participating in the OSPFv3 routing process.

Only the routers with the same instance ID can establish neighbor relationship one another.

After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3.

Examples

The following example starts the **OSPFv3** process on **int fastethernet 0/0** for the specified area of the specified instance.

```
int fastethernet 0/0
ipv6 ospf 1 area 2 instance 2
```

Related commands

Command	Description
ipv6 ospf prefix-filter	Set the prefix information not to be advertised on the interface.
ipv6 router ospf	Start the OSPFv3 routing process.
passive-interface	Set the passive interface.
show ipv6 ospf interface	Show the OSPFv3 interface information.

5.1.12 ipv6 ospf bdf

Use this command to enable or disable the BFD on the specifed OSPFv3 interface. The **no** form of this command is used to remove the setting on the interface..

ipv6 ospf bfd [**disable**] [**instance** *instance-id*]

no ipv6 ospf bfd [**instance** *instance-id*]

Parameter description

Parameter	Description
disable	Disable the BFD function on the specified OSPF interface.
instance *instance-id*	Configure the specified OSPFv3 instance on the interface, in the range of 0 to 255.

Default configuration N/A

Command mode Interface configuration mode.

Usage guidelines	The command **ipv6 ospf bfd** in the interface configuration mode takes precedence over the **bfd all-interfaces** command in the routing process configuration mode. You can use this command to enable the BFD on the specified interface according to the actual environment, also can use the command **bfd all-interfaces** in the OSPFv3 process configuration mode to enanble the BFD function on all OSPF interfaces and use the command **ip v6 ospf bfd disable** to disable the BFD on the specified interface.
Examples	N/A

Related commands

Command	Description
ipv6 router ospf *process-id*	Create the OSPFv3 routing process and enter into the routing process configuration mode.
bdf all-interfaces	Enable the BFD on all OSPFv3 interfaces.

5.1.13 ipv6 ospf cost

Use this command to set the cost of the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf cost *cost*[**instance** *instance-id*]

no ipv6 ospf cost[**instance** *instance-id*]

Parameter description

Parameter	Description
Cost	Cost of the interface. Its range is 1 to 65535, and the default value is 10.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration	10.

Command mode	Interface configuration mode.
Usage guidelines	By default, the cost of the interface is automatically calculated based on the bandwidth of the interface. You can also use this command to modify the cost of the interface, and it takes precedence over the metric value based on the reference bandwidth.
Examples	The following example sets the cost of the interface to 1: `ipv6 ospf cost 1`

Related commands

Command	Description
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

5.1.14 ipv6 ospf dead-interval

Use this command to set the interval for the interface to consider that the neighbor fails. If the interface does not receive the hello message from the neighbor, it considers that the neighbor fails. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	Interval of the neighbor fails. Its range is 1 to 65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration	Four times the value of **ip ospf hello-interval**.
Command mode	Interface configuration mode.

Usage guidelines	The dead time of neighbors shall be the same. Otherwise they cannot establish normal adjacency. By default, the dead interval is four times the hello interval. If the hello interval changes, the dead interval changes accordingly. It's not recommended to modify the parameters directly. If needed, note that: 1. The dead interval shall be larger than the hello interval sent by the neighbor. 2. The same dead interval shall be set for the neighbors.
Examples	The following example sets the dead interval of the local interface to 60s. `ipv6 ospf dead-interval 60`

Related commands

Command	Description
ipv6 ospf hello-interval	Set the interval for the interface to send the Hello message.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface

5.1.15 ipv6 ospf hello-interval

Use this command to set the interval for the interface to send the Hello message. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	Interval for sending the Hello message. Its range is 1-65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration	The broadcast network and point-to-point network :10 seconds. The point-to-multipoint network and NBMA network :30 seconds.

Command mode	Interface configuration mode.
Usage guidelines	The same hello interval must be set for the neighbors, otherwise they cannot establish normal adjacency.
Examples	The following example sets the interval for the interface to send the Hello message to 20s. `ipv6 ospf hello-interval 20`

Related commands

Command	Description
ipv6 ospf dead-interval	Set the interval for the interface to consider that the neighbor fails.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

5.1.16 ipv6 ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database description message. The **no** form of this command is used to restore it to the default.

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter description

Parameter	Description
instance *instance-id*	Configure the specific OSPFv3 instance on the interface, in the range of 0 to 255.

Default	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	After receiving the database description message, the device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database

	description message indicates an MTU greater than the interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.

Examples

The configuration example below disables the MTU check function on the interface ethernet 1/0.

```
DES-7200(config)# interface ethernet 1/0
DES-7200(config-if)# ipv6 ospf mtu-ignore
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
ipv6 mtu	Set the MTU of the IPv6.

5.1.17 ipv6 ospf neighbor

Use this command to set the OSPFv3 neighbor manually. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [**poll-interval** <0-2147483647> | **priority** <0-255>]] [**instance** *instance-id*]

no ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [**poll-interval** <0-2147483647> | **priority** <0-255>]] [**instance** *instance-id*]

Parameter description

Parameter	Description
cost <*1-65535*>	(Optional) Configure the cost to each neighbor in point-to-multipoint network. It is not defined by default, where the cost configured on the interface will be used. Only the point-to-multipoint type network supports this option.
poll-interval <*0*-2147483647>	(Optional) Interval to poll the neighbors (in seconds), 120 s by default. Only the non-broadcast (NBMA) type network supports this option.
priority <*0-255*>	(Optional) Configure the priority of non-broadcast network neighbors, 0 by default. Only the non-broadcast (NBMA) type network supports this option.

	instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Command mode	Interface configuration mode.

Usage guidelines	You can set relevant parameters for the neighbors depending on the actual network type.

5.1.18 ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf network {**broadcast | non-broadcast** | **point-to-point | point-to-multipoint** [**non-broadcast**]} [**instance** *instance-id*]

no ipv6 ospf network [**broadcast | non-broadcast** | **point-to-point | point-to-multipoint** [**non-broadcast**]] [**instance** *instance-id*]

Parameter description

Parameter	Description
broadcast	Specify the broadcast network type.
non-broadcast	Specify the non-broadcast network type.
point-to-point	Specify the point-to-point network type.
point-to-multipoint	Specify the point-to-multipoint network type.
point-to-multipoint non-broadcast	Specify the point-to-multipoint non-broadcast network type.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface with the valid id range of 0-255.

Default configuration	Point-to-point network type: PPP, SLIP, frame relay point-to-point sub-interface and X.25 point-to-point sub-interface encapsulation. NBMA network type: frame relay(except for the point-to-point sub-interface) and X.25 encapsulation (except for the point-to-point sub-interface) Broadcast network type: Ethernet encapsulation. The default network type is none point-to-multipoint network type.
Command mode	Interface configuration mode.
Usage guidelines	You can set the network type of the interface according to the actual link type and the topology.
Examples	The following example sets the network type of the interface that participates in the OSPFv3 to point-to-point. `ipv6 ospf network point-to-point`

Related commands

Command	Description
ipv6 ospf priority	Set the interface priority.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

5.1.19 ipv6 ospf priority

Use this command to set the interface priority. Use the **no** form of this command to restore the default setting.

ipv6 ospf priority *number-value* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter description

Parameter	Description
number-value	The priority of the interface. Its range is 0 to 255.
instance	Configure the specific OSPFv3

	instance-id	instance on the interface. Its range is 0 to 255.

Default configuration	1.
Command mode	Interface configuration mode.
Usage guidelines	In the broadcast type, it is necessary to elect the DR/BDR. In electing the DR/BDR, the device of the highest priority is preferred. If several devices are of the same priority, the one with the largest router-ID is preferred. The device with the priority level of 0 does not participate in the election of DR/BDR. If the DR and BDR are available in the network, modifying the interface priority will not take effect immediately. The interface will participate in the election of the DR/BDR at the next time.
Examples	The following example disables the interface from being elected as the DR/BDR. `ipv6 ospf priority 0`

Related commands

Command	Description
ipv6 ospf network	Set the network type of the interface.
router-id	Set the ID of the router.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

5.1.20 ipv6 ospf retransmit-interval

Use this command to set the interval for the interface to retransmit the LSA. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf retransmit-interval [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	Interval for retransmitting the LSA. Its range is 1 to 65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

5 seconds.

Command mode

Interface configuration mode.

Usage guidelines

To ensure the reliable transmission of routing information, the LSA sent to the neighbor shall be acknowledged by the neighbor. You can use this command to set the interval for waiting for the acknowledgement from the neighbor. If no acknowledgement is received within the specified period, the LSA information will be retransmitted.

Examples

The following example sets the interval for retransmitting the LSA to 10s.

```
ipv6 ospf retransmit-interval 10
```

Related commands

Command	Description
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

5.1.21 ipv6 ospf transmit-delay

Use this command to set the delay for the interface to sending the LSA. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]

no ipv6 ospf transmit-delay [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	The delay time for sending LSA. Its range is 1 to 65535(s).

	instance *instance-id*	Configure the specific OSPFv3 instance on the interface,0-255.

Default configuration

1 second.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to set the delay for the interface to transmit the LSA.

Examples

The following example sets the delay for the interface to transmit the LSA.

```
ipv6 ospf transmit-delay 2
```

Related commands

Command	Description
show ipv6 ospf interface	Show the OSPFv3 interface information.

5.1.22 ipv6 router ospf

Use this command to start OSPFv3 routing process. Use the **no** form of this command to disable the OSPFv3 routing process.

ipv6 router ospf *[process-id]*

no ipv6 router ospf *process-id*

Parameter description

Parameter	Description
process-id	OSPF process number. Without the process number configured, it indicates the process 1 is started.

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines	After the OSPFv3 process is started, the OSPFv3 configuration mode is entered. At present, our products support up to 32 OSPFv3 processes.
Examples	The following example starts the OSPFv3 process. `ipv6 router ospf 1`

Related commands

Command	Description
ipv6 ospf area	Configure the interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Show the OSPFv3 routing process information.

5.1.23 log-adj-changes

Use this command to enable the logging of the neighbor state changes. The **no** or **default** form of the command is used to disable it.

log-adj-changes

no log-adj-changes

Parameter settings	None
Default	By default, Disabled
Command mode	Routing process configuration mode

Examples	The configuration example below turns on the log for neighbor status change.
	`DES-7200(config)# router ospf 1`
	`DES-7200(config)# log-adj-changes detail`

Related commands

Command	Description
show ipv6 ospf	Show the OSPF global configuration information

5.1.24 max-concurrent-dd

Use this command to set the maximum number of DD packets that can be processed simultaneously.

max-concurrent-dd *number*

no max-concurrent-dd

	Parameter	Description
Parameter description	*number*	Maximum number of DD packets that can be processed simultaneously, 1-65535.

Default configuration	5
Command mode	Routing process configuration mode.

Examples	The following example set max-concurrent-dd to 4, allowing exchanging DD packet with 4 neighbors at the same time:
	`router ipv6 ospf 1`
	`max-concurrent-dd 4`

5.1.25 passive-interface

Use this command to set the passive interface. Use the **no** form of this command to remove the configuration .

passive-interface {**default** | *interface-type interface-number* }

no passive-interface {**default** | *interface-type interface-number* }

	Parameter	Description
Parameter description	**default**	Set all the interfaces to passive ones.
	interface-type interface-number	Set the specified interface to passive one.

Default configuration	None.

Command mode	OSPFv3 configuration mode.
Usage guidelines	After an interface is set to passive one, it no longer receives or sends the hello message. This command applies to the interfaces participating in the OSPF but not to the virtual links.

Examples	The following example enables only VLAN1 to participate in the OSPFv3 process.
	`passive-interface default`
	`no passive-interface vlan 1`

Related commands

Command	Description
ipv6 ospf area	Configure the interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.

5.1.26 redistribute

Use this command to start the route redistribution in order to import the routing information of other routing protocols to the OSPFv3 routing process. Use the **no** form of this command to disable this function or modify the redistribution parameters.

redistribute {**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**} [{**level-1** | **level-1-2** | **level-2**} **| match** {**internal | external** [**1|2**]**} | metric** *metric-value* **| metric-type** {*1*|*2*} | **route-map** *route-map-name* | **tag** *tag-value*]

no redistribute {**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**} [{**level-1** | **level-1-2** | **level-2**} **| match** {**internal | external** [**1|2**]**} | metric | metric-type** {*1*|*2*} | **route-map** *route-map-name* | **tag** *tag-value*]

Parameter description

Parameter	Description
bgp	The bgp protocol is redistributed.
connected	The directly connected route is redistributed.

isis*[area-tag]*	The isis is redistributed. The area-tag specifies the isis instance.
ospf *process-id*	The ospf is redistributed. The process-id specifies the ospf instance within the range of 1-65535.
rip	The rip is redistributed.
static	The static route is redistributed.
level-1| level-1-2| level-2	It is used in the IS-IS route redistribution only and redistributes the specified level route. By default, the level-2 route is redistributed.
metric *metric-value*	Specify the metric for the OSPFv3 external 2 LSA. Its range is 0 to 16777214.
metric-type *{1|2}*	Set the metric type for the external route to E-1 or E-2. The default type is E-2.
route-map *map-map-name*	Specify the routing policy for route redistribution. The name of **map-tag** can be up to 32 characters. No route-map is associated by default.
tag *tag-value*	Tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.
match	Redistribute the OSPF routes of the specific type: internal: inter-area and intra-area routes. external [1|2]: E1, E2 or all external routes. All sub-type OSPFv3 routes are redistributed by default.

Default configuration	Disabled.

Command mode	OSPFv3 configuration mode.
Usage guidelines	When a device supports multiple routing protocols, the coordination between these protocols becomes an important task. The device can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols. When redistributing OSPF routes, you can configure match to redistribute the corresponding routes. All types of OSPF routes are redistributed by default. The match parameter of route-map is specific the source of routes. The parameters *tag*, *metric* and *metric-type* of the set rule of route-map take precedence over the ones configured for the redistribute command. Caution: The metric value of the route-map associated should be in the range of 0 to 16777214. If the metric value is not in this range, the route can not be introduced.
Examples	The following example redistributes the direct route and associates route-map test (the corresponding rule is match metric 20 and set metric 20). `redistribute connect metric 10 route-map test`

Related commands

Command	Description
default-information originate	Set the default route to be redistributed.
default-metric	Set the default metric for the route to be redistributed.
summary-prefix	Set the converged address range of the external route.
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf database	Show the OSPFv3 LSA information.

5.1.27 router-id

Use this command to set the router ID (device ID). Use the **no** form of this command to remove the setting or restore it to the default router ID.

router-id *router-id*

no router-id

Parameter description

Parameter	Description
router-id	ID of the device in the IPv4 address format.

Default configuration

The best interface address is automatically selected as the router ID.

Command mode

OSPFv3 configuration mode.

Usage guidelines

Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the format of IPv4 address.

Unlike the OSPFv2, the OSPFv3 process will automatically acquire an IPv4 address to use it as the router ID. After the device starts the OSPFv3 process, a user must use the **router-id** command to configure the router ID for the OSPFv3 process. Otherwise, the OSPFv3 process will not be able to start.

The router ID shall be unique.

At present, after the OSPFv3 routing process starts, the Router ID shall be set before the interface participates in the OSPFv3. That is to say, after the interface runs OSPFv3 routing process, the router ID cannot be modified. Otherwise the OSPFv3 routing process and the whole OSPF AS will be greatly affected.

If the router ID needs to be reconfigured, shut down and restarts the OSPFv3 process, and then configure router ID.

Examples

The following example sets the ID of the device that participates in the OSPFv3 process to 1.1.1.1.

```
router-id 1.1.1.1
```

Related commands

Command	Description
ipv6 ospf priority	Set the interface priority.

	show ipv6 ospf	Show the OSPFv3 routing process information.

5.1.28 summary-prefix

Use this command to configure the converged route out of the OSPFv3 routing domain in the routing process configuration mode. The **no** form of this command is used to restore it to the default setting.

summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise | tag** <*0-4294967295*>]

no summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise | tag** <*0-4294967295*>]

Parameter description

Parameter	Description
ipv6-prefix/*prefix-length*	Address range of the converged route
tag<*0-4294967295*>	Tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.
not-advertise	Do not advertise the converged route.

Default No converged route is configured by default.

Command mode Routing process configuration mode.

Usage guidelines

When routes are redistributed by another routing process into the OSPFv3 routing process, every route is advertised to the OSPFv3-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous border device can advertise only one converged route, reducing the scale of routing table greatly.

Unlike the **area range** command, the former involves the convergence of routes between OSPFv3 areas, while the latter involves the convergence of external routes of the OSPFv3 routing domain.

	The **summary-address** command is valid only on the ASBR now, and causes the convergence for only redistributed routes.

Examples

The configuration command below configures the external route within the 2001:DB8::/64 to the converged route 2001:DB8::/64 to advertise it.

```
DES-7200(config-router)# summary-prefix 2001 :DB8 : : /64
```

Related commands

Command	Description
area-range	Configure route convergence between the OSPFv3 areas.
redistribute	Redistribute the route of other routing process.

5.1.29 timers spf

Use this command to set the delay and interval for the OSPFv3 to calculate SPF after receiving the topology change. The **no** format of this command is used to restore it to the default.

timers spf *delay holdtime*

no timers spf

Parameter description

Parameter	Description
delay	Delay from determining the topology change to calculating SPF. Its range is 0 to 214748364s, and the default value is 5s.
holdtime	Delay from determining the topology change to calculating SPF. Its range is 0 to 214748364s, and the default value is 5s.

Default configuration

spf-delay: 5 seconds.

spf-holdtime: 10 seconds.

Command mode

OSPFv3 configuration mode.

Usage guidelines	The smaller the *spf-delay* and *spf-holdtime*, the shorter time the OSPF takes to adapt to the topology change, but the more system space will be occupied.
Examples	`timers spf 2 4`

Related commands

Command	Description
clear ipv6 ospf	Restart part function of the OSPFv3.
show ipv6 ospf	Show the OSPFv3 routing process information.

5.1.30 timers throttle spf

Use this command to configure the topology change information for OSPFv3, including the delay for SPF calculation as well as the interval between two SPF calculations in the routing process configuration mode. The **no** form of this command restores it to the default.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter description

Parameter	Description
spf-delay	Define the SPF calculation waiting period, in milli-seconds, with the valid range from 1 to 600000. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Define the minimun interval between two SPF calculations, in milli-seconds, with the valid range from 1 to 600000.
spf-max-waittime	Define the maximum interval between two SPF calculations, in milli-seconds, with the valid range from 1 to 600000.

Default	spf-delay: 1000ms; spf-holdtime: 5000ms; spf-max-waittime: 10000ms.
Command mode	Routing process configuration mode.

Usage guidelines

Spf-delay refers to the delay time of the topology change to the SPF calculation. *Spf-holdtime* refers to the minimum interval between two SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval till it reaches to *spf-max-waittime*. If the interval between two SPF calculations has exceeded the required value, the SPF calculation will re-start from *spf-holdtime*.

Smaller *spf-delay* and *spf-holdtime* value can make the topology faster. Greater *spf-max-waittime* value can reduce the SPF calculation. Those configurations can be flexible according to the actual stability of the network topology.

Compared with the **timers spf** command, this command is more flexible. It not only speeds up the SPF calculation convergence, but also reduces the system resources consumption of SPF calculation due to the topology change. To this end, the **timers throttle spf** command is recommended.

Note

1. The spf-holdtime cannot be smaller than spf-delay, or the spf-holdtime will be set to be equal to spf-delay;
2. The spf-max-waitime cannot be smaller than spf-holdtime, or the spf-max-waittime will be set to be equal to spf-holdtime automatically;
3. The configurations of the **timers spf** command and the **timers throttle spf** command are overwritten.
4. Without neither **timers spf** command and **timers throttle spf** command configured, the default value refers to the one of the timers throttle spf command.

Examples

The configuration example below configures the delay and holdtime and the maximum time interval of the OSPFv3 as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculations are: 5ms，1s，3s，7s，15s，31s，63s，89s，179s，179+90 ……

```
DES-7200(config)# ipv6 router ospf 20
```

```
DES-7200(config-router)# timers spf 5 1000 90000
```

Related commands

Command	Description
show ipv6 ospf	Show the routing process information of the OSFPv3
clear ipv6 ospf	Restarts part OSPFv3 function.
timers spf	Configure the SPF calculation delay period.

5.2 Show Related Commands

5.2.1 show ipv6 ospf

Use this command to show the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter description

Parameter	Description
process- id	OSPF process number, 1-65535.

Command mode

Privileged mode.

Examples

The following example shows the information about the OSPFv3 process.

```
DES-7200# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 11
 Number of LSA received 4
 Log Neighbor Adjency Changes : Enabled
 Number of areas in this device is 2
 Area BACKBONE(0)
 Number of interfaces in this area is 1(1)
 SPF algorithm executed 4 times
 Number of LSA 3.  Checksum Sum 0x1DDF1
 Number of Unknown LSA 0
```

With the BFD for OSPFv3 configured, the content of "BFD is enabled" is added to the displaying information of the command **show ipv6 ospf**. For example:

```
DES-7200# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 11
 Number of LSA received 4
 Log Neighbor Adjency Changes : Enabled
 Number of areas in this device is 2
 BFD is enabled
 Area BACKBONE(0)
 Number of interfaces in this area is 1(1)
 SPF algorithm executed 4 times
 Number of LSA 3.  Checksum Sum 0x1DDF1
 Number of Unknown LSA 0
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
default-information originate	Set the default route to be redistributed.
default-metric	Set the default metric for the route to be redistributed.
router-id	Router ID
timers spf	Set the delay and interval for the OSPFv3 to perform SPF calculation after receiving the topology change.

5.2.2 show ipv6 ospf database

Use this command to show the database information of the OSPFv3 process

show ipv6 ospf [*process- id*] **database** [**lsa-type** [**adv-router** *router-id*]]

Parameter description

Parameter	Description
process- id	OSPF process number, 1-65535
lsa-type	LSA type. There are the following types: external, link, inter-prefix, inter-router, intra-prefix, network, router, te

	If this parameter is not specified, all LSA information will be shown.
adv-router *router-id*	Show the LSA information generated by the specified router.

Command mode

Privileged mode.

Examples

The following example shows the information about the OSPFv3 process database.

```
DES-7200# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface FastEthernet 1/0)

Link State ID   ADV Router     Age  Seq#      CkSum
Prefix
0.0.0.2       1.1.1.1        197 0x80000001 0x7cd8
0
0.0.0.5       2.2.2.2        206 0x80000001 0x8c86
0
              Link-LSA (Interface Loopback 1)
Link State ID   ADV Router     Age  Seq#      CkSum
Prefix
0.0.64.1      1.1.1.1         82 0x80000001 0xb760
0
              Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router     Age  Seq#      CkSum
Link
0.0.0.0       1.1.1.1      17 0x80000006 0x62a1     1
0.0.0.0       2.2.2.2        156 0x80000003 0x8653
1
              Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.5       2.2.2.2        157 0x80000001 0xf8f6
              Router-LSA (Area 0.0.0.1)
Link State ID   ADV Router     Age  Seq#      CkSum
Link
0.0.0.0       1.1.1.1         17 0x80000002 0x0529
0
              Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.1       1.1.1.1         77 0x80000002 0x83b4
AS-external-LSA
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.1       1.1.1.1         1 0x80000001 0x6035 E2
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.

5.2.3 show ipv6 ospf interface

Use this command to show the OSPFv3 interface information.

show ipv6 ospf interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and interface number.

Command mode

Privileged mode.

Examples

The following commands show the information about the OSPFv3 interface.

```
DES-7200# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

If the BFD has been enabled for the neighbor on the interface, the content of “BFD enabled” is added to the displaying information of the command **show ipv6 ospf interface**. For example:

```
DES-7200# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
```

```
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
ipv6 ospf area	Enable the interface to participate in the OSPFv3 process.

5.2.4 show ipv6 ospf neighbor

Use this command to show the neighbor information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **neighbor** [**interface-type** *interface-number* [**detail**]| *neighbor-id* |**detail**]

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1-65535
detail	Show details about the neighbor.
interface-type interface-number	Interface type And interface number
neighbor-id	Neighbor ID

Command mode

Privileged mode.

Examples

The following command shows the brief information about the OSPF neighbor.

```
DES-7200# show ipv6 ospf neighbor
OSPFv3 Process (1), Neighbores, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Interface
```

```
Instance ID
2.2.2.2         1   Full/DR       00:00:33
FastEthernet 1/0    0
```

The following command shows the details of neighbors:

```
DES-7200# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address
fe80::c800:eff:fe84:1c
   In the area 0.0.0.0 via interface FastEthernet 1/0
   Neighbor priority is 1, State is Full, 6 state changes
   DR is 2.2.2.2 BDR is 1.1.1.1
   Options is 0x000013 (-|R|-|-|E|V6)
   Dead timer due in 00:00:36
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
```

If the BFD detection has been enabled for the forwarding path of neighbor on the interface, the content of “BFD session state up” is added to the displaying information of the command **show ipv6 ospf neighbor detail**. For example:

```
DES-7200# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address
fe80::c800:eff:fe84:1c
   In the area 0.0.0.0 via interface FastEthernet 1/0
   Neighbor priority is 1, State is Full, 6 state changes
   DR is 2.2.2.2 BDR is 1.1.1.1
   Options is 0x000013 (-|R|-|-|E|V6)
   Dead timer due in 00:00:36
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
   BFD session state up
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
ipv6 ospf area	Enable the interface to participate in the OSPFv3 process.
area virtual-link	Configure the OSPFv3 virtual link.
show ipv6 ospf interface	Show the OSPFv3 interface information.

5.2.5 show ipv6 ospf route

Use this command to show the OSPFv3 route information.

show ipv6 ospf [*process- id*] **route** [**count**]

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1-65535.
count	Number of OSPFv3 routes

Command mode

Privileged mode.

Examples

The following example shows the information about OSPF routes.

```
DES-7200# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter
area, E1 - OSPF external type 1, E2 - OSPF external type
2
Destination                              Metric
Next-hop
E2 2222::/64                                    1/20
via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O  3333::/64                                     11
via fe80::c800:eff:fe84:1c, FastEthernet 1/0, Area
0.0.0.0
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.

5.2.6 show ipv6 ospf summary-prefix

Use this command to show the external rouitng convergence information of OSPFv3.

show ipv6 ospf [*process- id*] **summary-prefix**

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1-65535

Command mode

Privileged mode.

Examples

The following command shows the external routing convergence information of OSPFv3.

```
DES-7200# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:db8::/64,Metric 16777215,Type0,Tag0,Match count0,advertise
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
summary-prefix	Configure the converge route out of the OSPFv3 routing domain.

5.2.7 show ipv6 ospf topology

Use this command to show the topology of each area of OSPFv3.

show ipv6 ospf [*process- id*] **topology** [**area** *area-id*]

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1-65535
area-id	Area ID

Command mode

Privileged mode.

Examples

The following command shows the topology of each area of OSPFv3.

```
DES-7200# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID       Bits  Metric    Next-Hop
Interface
1.1.1.1          EB  --
2.2.2.2          E   1         2.2.2.2
FastEthernet 1/0

OSPFv3 paths to Area (0.0.0.1) routers
Router ID       Bits  Metric    Next-Hop
Interface
1.1.1.1          B   --
```

	Command	Description
Related commands	**ipv6 router ospf**	Start the OSPFv3 routing process.
	area range	Configure the address range of the OSPF area.

5.2.8 show ipv6 ospf virtual-links

Use this command to show the virtual link information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **virtual-links**

	Parameter	Description
Parameter description	*process- id*	OSPFv3 process number, 1.65535

Command mode	Privileged mode.

Examples

The following command shows the information about the OSPFv3 virtual link.

```
DES-7200# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 2.2.2.2 is down
  Transit area 0.0.0.1 via interface FastEthernet 1/0,
instance ID 0
  Local address *
  Remote address 3333::1/128
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in inactive
    Adjacency state Down
```

	Command	Description
Related commands	**ipv6 router ospf**	Start the OSPFv3 routing process.
	area virtual-link	Configure the OSPFv3 virtual link.
	show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.

6 BGP4 Commands

6.1 Configuration Related Commands

6.1.1 address-family ipv4

Use this command to enter " **address-faimly IPv4**" to configure the BGP configuration mode. Use the **exit-address-family** command to exit the BGP address configuration mode.

address-family ipv4 [**unicast**]

no address-family ipv4 [**unicast**]

Parameter description

Parameter	Description
unicast	Optional, detailed IPv4 unicast address prefix

Default configuration

Unicast address prefix.

Command mode

BGP configuration mode.

Usage guidelines

In the BGP address configuration mode, the standard IPv4 address can be used for the configuration.

To exit to the BGP configuration mode, run the command **exit-address-family**

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# address-family ipv4
```

Related commands

Command	Description
exit-address-family	Exit the mode.

6.1.2 address-family ipv4 vrf

Use this command to enter the address-family IPv4 VRF configuration mode to configure BGP and enable the exchange of route information of a VRF. Use the **no** form of this command to disable the exchange function or the **exit-address-family** command to exit the BGP address configuration mode.

address-family ipv4 vrf *vrf-name*

no address-family vrf *vrf-name*

Parameter description

Parameter	Description
vrf-name	VRF name

Default configuration

No vrf is defined by default.

Command mode

BGP configuration mode.

Usage guidelines

You can execute this command to configure or exit the exchange of route information between PEs and CEs.

To exit to the BGP configuration mode, run the **exit-address-family** command**.**

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# address-family ipv4 vrf vpn1
```

Related commands

Command	Description
exit-address-family	Exit the configuration mode.

6.1.3 address-family ipv6

Use this command to enter " **address-faimly IPv6**" of the BGP configuration mode and enable the exchange of IPv6 route information. The **no** form of this command disables this function. Use the **exit-address-family** command to exit the BGP address-family configuration mode.

address-family ipv6 [**unicast | multicast**]

no address-family ipv6 [**unicast | multicast**]

Parameter description

Parameter	Description
unicast	Optional, enter the IPv6 unicast

	address-family configuration mode.
multicast	Optional, enter the IPv6 multicast address-family configuration mode.

Default configuration

Unicast address prefix.

Command mode

BGP configuration mode.

Usage guidelines

You can use this command not only to enter the IPv6 address-family configuration mode of the BGP to configure the IPv6 neighbors ,but also activate neighbors in the IPv6 address-family configuration mode after configuring the IPv6 neighbors in the BGP configuration mode.

You can enter the multicast mode to configure the BGP of the multicast topology, which is used for the RPF detection of the IPv6 multicast routing protocol.

The **exit-address-family** command is used to exit to the BGP configuration mode.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# address-family ipv6
```

Related commands

Command	Description
exit-address-family	Exit the mode.

6.1.4 address-family vpnv4

Use this command to enter the address-family VPN configuration mode and enable the exchange of VPN route information between PE peers. Use the **exit-address-family** command to exit the BGP address configuration mode.

address-family vpnv4 [**unicast**]

no address-family vpnv4 [**unicast**]

Parameter description

Parameter	Description
unicast	Optional, detailed IPv4 unicast address prefix

Default

No VPN address family is defined by default.

configuration	
Command mode	BGP configuration mode.
Usage guidelines	Execute this command to enter the address-family VPN configuration mode and enable the exchange of VPN route information between PE peers. To exit to the BGP configuration mode, run the command **exit-address-family**
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# address-family vpnv4`

Related commands

Command	Description
exit-address-family	Exit the mode.

6.1.5 aggregate-address (IPv4)

Use this command to set the aggregate IPv4 route. The **no** form of the command is used to disable this function.

aggregate-address *ip-address mask* [**as-set**] [**summary-only**]

no aggregate-address *ip-addres mask* [**as-set**] [**summary-only**]

Parameter description

Parameter	Description
ip address	IP address of the aggregate route
mask	Mask of the aggregate route
as-set	Keep the AS path information of the path in the aggregate address range.
summary-only	Advertise only the aggregate route.

Default configuration	N/A.
Command mode	BGP configuration mode, address-family IPv4 configuration mode, address-family IPv4 VRF configuration mode.
Usage	By default, the BGP-enabled device will advertise all path

guidelines	information both before and after aggregation. If you only hope to advertise the aggregate route, use the **aggregate-address summary-only** command.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# aggregate-address 10.0.0.0
255.0.0.0 as-set
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.

6.1.6 aggregate-address (IPv6)

Use this command to set the aggregate IPv6 route. The **no** form of the command is used to disable this function.

aggregate-address *ipv6-network / length* [**as-set**] [**summary-only**]

no aggregate-address *ipv6-network / length* [**as-set**] [**summary-only**]

Parameter description

Parameter	Description
ipv6-network	IP address prefix of the aggregate route
length	Length of the aggregate route
as-set	Keep the AS path information of the path in the aggregate address range.
summary-only	Advertise only the aggregate route.

Default configuration	N/A.
Command mode	BGP IPv6 address-family configuration mode
Usage guidelines	By default, the BGP-enabled device will advertise all path information both before and after aggregation. If you only hope to advertise the aggregate route, use the **aggregate-address summary-only** command.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# address-family ipv6
DES-7200(config-router-af)# aggregate-address 2008::/90
```

	as-set

Related commands	Command	Description
	router bgp	Enable the BGP protocol.

6.1.7 bgp always-compare-med

Use this command to compare Multi Exit Discriminator (MED) all the time. You can use the **no** form of the command to disable this function.

bgp always-compare-med

no bgp always-compare-med

Parameter description	N/A.
Default configuration	By default, the MED of the peer path from the same AS is compared.
Command mode	BGP configuration mode.
Usage guidelines	By default, the MED value is compared for the path of the peer from the same AS. If you hope to allow comparing MED values for the paths from different ASs, this command can be used. If there are multiple valid paths to the same destination, the one with lower MED value has higher priority. Unless you are sure that the different ASs are using the same IGP and routing method, this command is not recommended.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# bgp always-compare-med`

Related commands	Command	Description
	show ip bgp	Show the BGP route entry.
	bgp bestpath med confed	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.

bgp bestpath med missing-as-worst	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp deterministic-med	Compare the path of the peer from the same AS while selecting the optimal path.

6.1.8 bgp asnotation dot

Use this command to modify the showing mode of the 4-byte AS notation and the matching type of the regular expression as the dot mode(that is, two dotted decimal numbers). You can use the **no** form of the command to disable this function.

bgp asnotation dot

no bgp asnotation dot

Parameter description	N/A.
Default configuration	By default, the 4-byte AS notation is shown in decimal digit, and the regular expression matches the 4-byte AS notation with decimal digit too.
Command mode	BGP configuration mode.
Usage guidelines	Our devices support two modes of representing the 4-byte AS notation. One is decimal digit, and another is dot mode which represents the 65536 with 1.0. The decimal format is same as the default format, which represents the 4-byte AS notation with decimal digits. The dot mode shows the 4-byte AS notation in the format of ([two high bytes.] two low bytes). If the [two high bytes.] is zero, it will not be shown. That is, the AS notation represented as 65536 in decimal is 1.0 in the dot mode. Such as another example, the AS notation is 65534 represented in decimal, while it is represented as 65534 in the dot mode without the zero in front. No matter which mode will be adopted to show the 4-byte AS notation, both the two modes can be used when entering the configuration commands. But the representation and showing mode of the 4-byte AS notation

in the regular expression must be the same. Otherwise, the matching will fail.

After executing the **bgp asnotation** command, you must use the **clear ip bgp** * perform the resetting, so as to re-match the filtering condition of the regular expression.

Caution The AS notation is represented as 1 to 65535 no matter using decimal or dot mode.

Examples

```
DES-7200(config)# router bgp 1.0
DES-7200(config-router)# bgp asnotation dot
```

Related commands

Command	Description
show ip bgp summsry	Show the related information of BGP neighbor.

6.1.9 bgp bestpath as-path ignore

Use this command to disregard the length of the AS path. You can use the **no** form of the command to disable this function.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Parameter description N/A.

Default configuration By default, the AS path length is considered in choosing the optimal path.

Command mode BGP configuration mode.

Usage guidelines The BGP will not take the length of the AS path into account when it selects the optimal path as specified in RFC1771. In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# bgp bestpath as-path ignore
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

6.1.10 bgp bestpath compare-confed-aspath

Use this ocmmand to compare the AS path length of the confederation from the same external routes during selecting the optimal path, with smaller AS path in the confederation for higher path priority. You can use the **no** form of the command to disable this function.

bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

Parameter description

N/A.

Default configuration

By default, the AS path of the ebgp peer routes inside the same confederation is not compared during selecting the optimal path. Instead, the routing method is implemented.

Command mode

BGP configuration mode.

Usage guidelines

By default, during the selection of the same routing information from the peer of the internal EBGP, the AS path of the confederation is not compared. This command is used to compare the AS path of the confederation.

Note that if a route does not contain the AS path of the confederation, it is not possible to implement the AS path comparison for that route.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# bgp bestpath
compare-confed-aspath
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

	bgp router-id	Set the BGP Device ID.

6.1.11 bgp bestpath compare-routerid

Use this command to compare the router ID of the same external routes during selecting the optimal path, with smaller router ID for higher path priority. You can use the **no** form of the command to disable this function.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Parameter description	N/A.
Default configuration	By default, if two paths received from different EBGP peers have the same path, the first one is considered with higher priority.
Command mode	BGP configuration mode.
Usage guidelines	By default, if two paths with full identical path attributes are received from different EBGP Peers during the selection of the optimal path, we will select the optimal path according to the sequence of receiving the paths. You can select the path with smaller Device ID as the optimal path by configuring the following commands.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# bgp bestpath compare-routerid`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp router-id	Set the BGP Device ID.

6.1.12 bgp bestpath med confed

Use this command to compare the MED value of the path of the internal peer from AS confederation during selecting the optimal path. You can use the **no** form of the command to disable this function.

bgp bestpath med confed [missing-as-worst]

no bgp bestpath med confed [missing-as-worst]

Parameter description

Parameter	Description
missing-as-worst	Set the priority of the path without MED attribute as the lowest.

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

The MED attribute of the path is transferred between the ASs inside the confederation. You may set always comparing this value.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# bgp bestpath med confed
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp always-compare-med	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.
bgp bestpath med missing-as-worst	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp deterministic-med	Compare the path of the peer from the same AS while selecting the optimal path.

6.1.13 bgp bestpath med missing-as-worst

Use this command to set the priority of the path without MED attribute as the lowest while selecting the optimal path. You can use the **no** form of the command to disable this function.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

Parameter description	N/A.
Default configuration	By default, if a path without MED attribute is received, the MED value of the path is considered as 0. This kind of routes has the highest priority according to the known rule.
Command mode	BGP configuration mode.
Usage guidelines	By default, if the path whose MED attribute is not set is received, the MED value of this path will be taken as 0. For the smaller the MED value, the higher the priority of the path is, the MED value of this path reaches the highest priority. If you hope the path without MED attribute configured has the lowest priority, this command can be used.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# bgp bestpath med missing-as-worst`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp always-compare-med	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.
bgp bestpath med confed	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp deterministic-med	Compare the path of the peer from the same AS while selecting the optimal path.

6.1.14 bgp client-to-client reflection

Use this command to enalbe the route reflection function between clients on the device. The **no** form of the command disables the route reflection function between clients.

bgp client-to-client reflection

no bgp client-to-client reflection

Parameter description	N/A.
Default configuration	Enabled without the client for route reflection
Command mode	BGP configuration mode.
Usage guidelines	In general, it is not necessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the route among clients. However, if the full connection relationship is established for all clients, the function for the route reflector to reflect the client route can be disabled. To disable the route reflection function, use the command **no bgp client-to-client reflection**.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# no bgp client-to-client reflection`

Related commands

Command	Description
bgp cluster-id	Configure the cluster ID of the route reflector.
neighbor route-reflector-client	Configure the client of the route reflector and configure itself as the route reflector.

6.1.15 bgp cluster-id

Use this command to configure the cluster ID of the route reflector. Use the **no** form of the command to restore it to the default setting.

bgp cluster-id *cluster-id*

no bgp cluster-id

Parameter description

Parameter	Description
cluster-id	Cluster ID of the route reflector, an IP address of up to four bytes or an integer (must be entered in form of

	IP address).

Default configuration	N/A.
Command mode	BGP configuration mode.
Usage guidelines	In general, one group is only configured with one route reflector. In this case, the Device ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# bgp cluster-id 10.0.0.1`

Related commands

Command	Description
bgp client-to-client reflection	Configure the route reflection between clients.
neighbor route-reflector-client	Configure the client of the route reflector and configure itself as the route reflector.

6.1.16 bgp confederation identifier

Use this command to configure the AS confederation identifier. Use the **no** form of the command to restore it to the default setting.

bgp confederation identifier *as-number*

no bgp confederation identifier

Parameter description

Parameter	Description
as-number	AS confederation identifier in the range of 1 to 65535

Default configuration	N/A.

Command mode	BGP configuration mode.
Usage guidelines	The confederation is a measure to reduce the connections of the IBGP peer within the AS. One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.
Examples	`DES-7200(config-router)# bgp confederation identifier 65000`

Related commands

Command	Description
bgp confederation peers	Add member AS of the AS confederation.

6.1.17 bgp dampening

Use this command to enable the routing attenuation and set the attenuation paramters in the address-family or routing configuration mode. The **no** form of this command is used to remove the setting.

bgp dampening [*half-life* [*reusing supressing duration*] | **route-map** *name*]

no bgp dampening [*half-life* [*reusing suppressing duration*] **| route-map** [*name*]]

Parameter description

Parameter	Description
half-life	Half-life period, in minute, ranging from 1 to 45 minutes.
reusing	When the penalty value reaches this value, the routing suppression is cancelled. The value ranges from 1 to 20000.

suppressing	When the penalty value reaches this value, the routing suppression is performed. The value ranges from 1 to 20000.
duration	The maximum time for routing suppresion, ranging from 1 to 255 minutes.
name	Route-map name, apply the routing attenuation to the specified route through the route-map.

Default configuration Disabled.

Command mode BGP configuration mode, BGP IPv4 address-family configuration mode, BGP IPv4 VRF address-family configuration mode

Usage guidelines The bgp dampening command is used to suppress the unstable BGP routing. The BGP uses the penalty value to describe the routing suppression intensity. The penalty value increases 1000 when the routing oscillation is performed once. The suppressed routes will not be used during the BGP routing election.

Examples

```
DES-7200(config-router)# bgp dampening 30 1500 10000 120
```

Related commands

Command	Description
clear ip bgp dampening	Clear the BGP suppression and cancel the suppression for the routes.
show ip bgp dampening dampened-paths	Show the suppressed route information.

6.1.18 bgp confederation peers

Use this command to configure the member AS of the AS confederation. The **no** form of the command deletes the configured member AS.

bgp confederation peers *as-number* […*as-number*]

no bgp confederation peers *as-number* […*as-number*]

Parameter description

Parameter	Description
as-number	Member AS in the confederation In the range of 1 to 65535. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is 1 to 4294967295, which is represented as 1 to 65535.65535 in dot mode.

Default configuration

N/A.

Command mode

BGP configuration mode.

Usage guidelines

The confederation is a measure to reduce the connections of the IBGP peer within the AS.

One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.

This command is used to specify the member AS of a confederation.

Note: This command can configure up to 15 members of a confederation at one time. For more members, enter them for several times.

Examples

```
DES-7200(config-router)# bgp confederation peers 65000
65100
```

Related commands

Command	Description
bgp confederation identifier	Configure the confederation identifier.

6.1.19 bgp default ipv4-unicast

Use this command to set the IPv4 unicast address as the default address family. The **no** form of the command removes the configuration.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Parameter description

N/A.

Default configuration

By default, the IPv4 unicast address is the default address family.

Command mode

BGP configuration mode.

Usage guidelines

This command is used to set the default address family of BGP as the IPv4 unicast address.

Examples

```
DES-7200(config-router)# default ipv4-unicast
```

Related commands

Command	Description
address-family ipv4	Enter the IPv4 address mode.

6.1.20 bgp default local-preference

Use this command to set the default local-preference attribute value. Use the **no** form of the command to restore the defaults.

bgp default local-preference *value*

no bgp default local-preference

Parameter description

Parameter	Description
value	Local priority attribute in the range 0 to 4294967295

Default configuration	100.
Command mode	BGP configuration mode.
Usage guidelines	The BGP takes the local preference as the foundation to compare with the priority of the path learned from the IBGP peers. The larger the local preference value, the higher the priority of the path is. The BGP speaker sends the external route received to the IBGP peers to add the local priority value.
Examples	`DES-7200(config-router)# bgp default local-preference 200`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp always-compare-med	In electing the optimal path, allow comparing the MED value of the path of the peer from different ASs.
bgp bestpath med confed	In electing the optimal path, allow comparing the MED value of the path of the internal peer from AS community.
bgp bestpath med missing-as-worst	In electing the optimal path, allow setting the priority of the path without MED attribute as the lowest.

6.1.21 bgp default route-targe filter

Use this command to enable the route-targe filtering. For the VPNV4 routes, filter the community attributes of the route-targe by default. Use the **no** form of the command to disable this function.

bgp default route-targe filter

no bgp default route-targe filter

Default configuration	Enabled.
Command mode	BGP configuration mode.
Usage guidelines	After receiving the VPNV4 route, use the community attributes list of the route-targe to implement the filtering and distribute to different VRFs. With the **no** form of this command used, the BGP will receive all VPNV4 routes no matter whether these filtered VPNV4 routes will be received by route-targe of local VRF. With the PE route-reflector-client configured for the BGP, the handling to the VPNV4 route is executed by the way without the route-targe filtering. In this case, whether the BGP is enabled, the actions are the same without the route-targe filtering.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# no bgp default route-targe filter`

Related commands

Command	Description
neighbor route-reflector-client	Configure the route-reflector-client, and set itself as the route reflector.

6.1.22 bgp deterministic-med

This command sets comparing preferentially the MED values of peer paths from the same AS. By default, the comparison is based on the received order, and the one received the last is compared first. The **no** format of the command turns off it.

bgp deterministic med

no bgp deterministic med

Parameter description	N/A.
Default configuration	By default, the function is disabled.

Command mode	BGP CONFIGURATION MODE.
Usage guidelines	By default, they will be compared with each other according to the sequence the paths are received when the optimal path is selected. If you hope to compare with the path of the peers from the same AS firstly, execute the following operations in the BGP configuration mode:
Examples	`DES-7200(config-router)# bgp deterministic med`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp always-compare-med	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.
bgp bestpath med confed	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp bestpath med missing-as-worst	Compare the path of the peer from the same AS while selecting the optimal path.

6.1.23 bgp enforce-first-as

Use this command to reject the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number. The **no** format of the command disables the function.

bgp enforce-first-as

no bgp enforce-first-as

Parameter description	N/A.
Default configuration	Enabled
Command mode	BGP configuration mode.

Usage guidelines	By default, the AS number of the device is put into the path section for updating the update message.

Examples

```
DES-7200(config-router)# bgp enforce-first-as
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

6.1.24 bgp fast-external-fallover

When the network interface that is used in establishing the connection of the directly-connected EBGP peer fails, this command is used to establish the BGP session connection quickly. You can use the **no** form of the command to disable this function.

bgp fast-external-fallover

no bgp fast-external-fallover

Parameter description	N/A.
Default configuration	Enabled.
Command mode	BGP configuration mode.
Usage guidelines	This command takes effect only for the directly-connected EBGP neighbor.

Examples

```
DES-7200(config-router)# bgp faster-external-fallover
```

Related commands

Command	Description
router bgp	Enabled the BGP protocol.

6.1.25 bgp graceful-restart

Use this command to enable the graceful restart function of the globla BGP. The **no** form of the command is used to disable this function.

bgp graceful-restart

no bgp graceful-restart

Default	Disabled.
Command mode	BGP configuration mode.
Usage guidelines	The ability of the BGP is advertised and negotiated through the ability field of the Open message. The negotiation of the ability is implemented during initially setting up the connection. So both sides must reach the consistency of the ability. Not supported by any side will lead to this router device performing the GR incorrectly. With the GR function enabled, the connected Open message will carry the GR ability field to perform the negotiation of the GR ability. To implement the GR correctly, the GR function must be enabled on the both sides of the neighbors. This command does not take effect immediately on all BGP connections that are set up successfully. So if you want these BGP connections to negotiate the GR ability immediately, you need to restart the BGP connection forcibly to make the local device negotiate the GR ability with the Peer again. The BGP graceful-restart is used to implement the continuous data forwarding of the whole network, it requires the device to keep the BGP routing entry valid and go on performing the data forwarding when restarting the BGP protocol. Supporting the continuous forwarding during the restarting is related to the hardware ability.
Examples	`DES-7200(config)# router bgp 500` `DES-7200(config-router)# bgp graceful-restart`

Related commands

Command	Description
router bgp	Enable the BGP protocol.
bgp graceful-restart restart-time	Configure the restart time of the BGP graceful-restart.

6.1.26 bgp graceful-restart restart-time

Use this command to configure the restart time of the BGP graceful-restart. The **no** form of the command restores it to the default value.

bgp graceful-restart restart-time *restart-time*

no bgp graceful-restart restart-time

Parameter description

Parameter	Description
restart-time	GR Restarter-hoped longest waiting time before re-establishing the connection between the GR Helper and the GR Restarter, in the range of 1 to 3600 seconds.

Default

120 seconds.

Command mode

BGP configuration mode.

Usage guidelines

The restart time is advertised by the GR Restarter to the GR Helper, it is the GR Restarter-hoped longest waiting time before re-establishing the connection between the GR Helper and the GR Restarter. After this time, if the BGP connection with the GR Restarter has not been the Established status, the GR Helper will consider this BGP session fails and perform the normal BGP restoring.

The restart time is advertised in the GR ability field of the BGP Open message. The GR restart time of the two ends of the session is not required to be the same ,but it is recommended.

Examples

```
DES-7200(config)# router bgp 500
DES-7200(config-router)# bgp graceful-restart
DES-7200(config-router)# bgp graceful-restart restart-time 150
DES-7200(config-router)# no bgp graceful-restart restart-time
```

Related commands

Command	Description
bgp graceful-restart	Enable the BGP graceful-restart.

6.1.27 bgp graceful-restart stalepath-time

Use this command to confugre the time to help the device keep the route valid when executing the BGP graceful-resatart. The **no** form of the command restores the stalepath-time to the default value.

bgp graceful-restart stalepath-time *stalepath-time*

no bgp graceful-restart stalepath-time

Parameter description

Parameter	Description
time	Longest time used to keep the stale route valid after restoring the connection with the neighbors, in the range of 1 to 3600 seconds.

Default

360 seconds.

Command mode

BGP configuration mode.

Usage guidelines

This command is configured for the parameters of the GR Helper. The stalepath-time is the longest time of the GR Helper waiting to receive the EOR mark of the Restarter after restoring the connection with the GR Restarter. When the GR Helper detects that the connection with the GR Restarter breaks, the original route of the Restarter is marked as the “Stale”, however these routes are still used for the routing calculation and forwarding.

The GR Helper updates the routes and cancels the “Stale” mark according to route updating information received from the GR Restarter. If these routes with the “Stale” mark are not updated in the stalepath-time period, they will be deleted. This mechanism is used to avoid the unable convergence of routes when the GR Helper does not receive the EOR mark of the GR Restarter for a long time.

Examples

```
DES-7200(config)# router bgp 500
DES-7200(config-router)# bgp graceful-restart
DES-7200(config-router)# bgp graceful-restart
stalepath-time 240
DES-7200(config-router)# no bgp graceful-restart
stalepath-time
```

Related commands

Command	Description
bgp graceful-restart	Enable the BGP graceful-restart .

6.1.28 bgp log-neighbor-changes

Use this command to log the BGP status changes without turning on **debug**. You can use the **no** form of the command to disable this function.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Parameter description N/A.

Default configuration Disabled.

Command mode BGP configuration mode.

Usage guidelines The **debug** command can also be used to log the BGP status changes. But this command may consume a great deal of resources.

Examples

```
DES-7200(config-router)# bgp log-neighbor-changes
```

Related commands

Command	Description
router bgp	Enabled the BGP protocol.

6.1.29 bgp nexthop trigger delay

Use this command to configure the delay time of updating the routing table when the nexthop of the BGP route changes . You can use the **no** form of the command to restore it to the default setting.

bgp nexthop trigger delay *delay-time*

no bgp nexthop trigger delay

Parameter description

Parameter	Description
delay-time	Delay time of updating the routing table when the nexthop changes, in the range of 0 to 100 seconds.

Default configuration

5 seconds.

Command mode

BGP configuration mode, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command is used to configure the delay time of updating the routing table when the nexthop changes, it takes effect with the **bgp nexthop trigger enable** configured.

Examples

```
DES-7200(config-router)# bgp nexthop trigger delay 30
```

Related commands

Command	Description
bgp nexthop trigger enable	Enable the nexthop trigger.

6.1.30 bgp nexthop trigger enable

Use this command to enable the nexthop trigger update function. You can use the **no** form of the command to disable this function.

bgp nexthop trigger enable

no bgp nexthop trigger enable

Parameter description

N/A.

Default configuration

Enabled.

Command mode

BGP configuration mode, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF

	configuration mode.
Usage guidelines	This command is used to enable the nexthop trigger update function.
Examples	`DES-7200(config-router)# bgp nexthop trigger enable`

Related commands

Command	Description
Bgp nexthop trigger delay	Set the delay time of updating the routing table when the nexthop changes.

6.1.31 bgp redistribute-internal

Use this command to control the BGP whether to allow to redistribute the routes learned from the IBGP to the IGP protocol,such as RIP, OSPF, ISIS,etc.

bgp redistribute-internal

no bgp redistribute-internal

Parameter description	N/A.
Default configuration	By default, the IBGP route is allowed to be redistributed to the IGP protocol.
Command mode	BGP configuration mode, address-family IPv4/IPv6 configuration mode, address-family IPv4 VRF configuration mode.
Usage guidelines	This command is used to control the IBGP route whether to be allowed to be redistributed to the IGP protocol.
Examples	`DES-7200(config-router)# bgp redistribute-internal`

Related commands

Command	Description
redistribute	Redistribute the routes learned from other protocols.

6.1.32 bgp router-id

Use this command to configure the ID-IP address of the device. The **no** form of the command restores it to the default IP address.

bgp router-id *ip-address*

no bgp router-id

Parameter description

Parameter	Description
ip address	IP address

Default configuration

By default, the loop-back interface of the device is selected preferentially. If it does not exist, the device ID of the device is used.

Command mode

BGP configuration mode.

Usage guidelines

This command is used to configure the ID-IP address of the device used in running the BGP protocol.

Examples

```
DES-7200(config-router)# bgp router-id 10.0.0.1
```

Related commands

Command	Description
show ip bgp dampening dampened-paths	Show the suppressed routing information.
bgp dampening	Enable the route dampening function and set the dampening parameters.

6.1.33 bgp scan-rib disable

Use this command to configure the the timely scan for the BGP protocol to update the routing table. The **no** form of this command cancels the timely scan.

bgp scan-rib disable

no bgp scan-rib disable

Default configuration

Disabled.

Command mode	BGP configuration mode, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF configuration mode.
Usage guidelines	N/A
Examples	`DES-7200(config-router)# bgp scan-rib disable`

Related commands

Command	Description
bgp scan-time	Configure the interval of the BGP timely scan.

6.1.34 bgp scan-time

Use this command to configure the interval of the BGP timely scan.

bgp scan-time *time*

no bgp scan-time [*time*]

Parameter description

Parameter	Description
time	Interval of the timely scan, in the range of 5 to 60 seconds.

Default configuration	60 seconds.
Command mode	BGP configuration mode, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF configuration mode.
Usage guidelines	This command is used to configure the interval of the BGP timely scan; it takes effect when the **bgp scan-rib enable** is configured.
Examples	`DES-7200(config-router)# bgp scan-time 30`

Related

Command	Description

	bgp scan-rib enable	Enable the BGP updating the routing table with the timely scan..

6.1.35 bgp update-delay

Use this command to set the maximum delay time of the BGP Speaker first sending the updating information to neighbors. The **no** form of the command restores it to the default value. During the BGP graceful-restart, this command is used to update the delay time.

bgp update-delay *delay-time*

no bgp update-delay

	Parameter	Description
Parameter description	*delay-time*	Maximum delay time of the BGP Speaker sending its route updating information, in the range of 0 to 3600 seconds, 120 seconds by default. For the BGP graceful-restart, it is the maximum time of waitng to receive the EOR message of all neighbors, in the range of 1 to 3600 seconds.

Default configuration	120 seconds.
Command mode	BGP configuration mode.
Usage guidelines	With the BGP starting up, it first waits some time to establish the connection with its neighbors, and then sends the updating message to these neighbors. After connecting with neighbors, the BGP does not send the updating message to them immediately, but waits some time to fully receive the updating routing message from all neighbors and then performs the routing optimization calculation and finally advertises the route updating message to its neighbors, which improves the convergence time and reduces the calculation consumption. If the software sends the route updating information to its neighbors immediately, it may send the information again due to receiving the more optimized

routes from other neighbors.

The **bgp update-delay** command is used to adjust the software's the initial waiting time, which is the maximum time, from establishing the connection with the first neighbor to performing the routing optimization calculation and sending the route advertisement. When the BGP graceful-restart is enabled, this command is also used to set the maximum time of waiting to receive the EOR messages from all neighbors. This value could be set properly larger if the neighbors are too many or the routing information of the neighbors is too much.

Examples

The following example sets the update-delay time as 200 seconds.

```
DES-7200(config)# router bgp 500
DES-7200(config-router)# bgp graceful-restart
DES-7200(config-router)# bgp update-delay 200
```

Related commands

Command	Description
bgp graceful-restart	Enable the BGP graceful-restart.

6.1.36 clear bgp all

Use this command to reset all BGP adderss-families. The content to be reset depends on the parameters behind.

clear bgp all [*as number*]

clear bgp all peer-group *peer-group-name* [[**soft**] [**in** | **out**]]

Parameter description

Parameter	Description
none parameter	Reset the peer sessions in all address-family.
as number	Reset the sessions with all members in the specified AS.
peer-group	Reset the specified peer group.
peer-group-name	Name of the peer group.
in	Perform soft resetting for the received routing information.
out	Perform soft resetting for the redistributed routing information.

	soft	Perform soft resetting for all routing information received/sent from/to the specified peer
	soft in	Perform soft resetting for the received routing information.
	soft out	Perform soft resetting for the distributed routing information.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is used to reset the sessions of all supported address-families, also including the vrf session in every address-family. This command is used to reset the sessions of all supported address-families, also including the vrf session in every address-family.

Examples N/A

Related commands

Command	Description
clear bgp ipv4 unicast	Perform the resetting for the IPv4 unicast address-family.

6.1.37 clear bgp ipv4 mdt

Use this command to reset the IPv4 mdt address-family of BGP. This command has the similar function with the clear bgp ipv4 unicast command except for the operation address family.

Parameter description

Parameter	Description
Refer to the clear bgp ipv4 unicast command.	Refer to the clear bgp ipv4 unicast command.

Default configuration Refer to the clear bgp ipv4 unicast command.

Command mode	Privileged mode.
Usage guidelines	Refer to the clear bgp ipv4 unicast command.
Examples	N/A

Related commands

Command	Description
clear bgp ipv4 unicast	Perform the resetting for the IPv4 unicast address-family.

6.1.38 clear bgp ipv4 unicast

Use this command to reset the BGP.

clear bgp ipv4 unicast {* |*address* | *as number* } [[**soft]** [**in** | **out**]]

Parameter description

Parameter	Description
*****	Reset all the current BGP sessions, and the BGP OVERFLOW state.
address	Reset the BGP session with the specified peer.
as number	Reset the sessions with all members in the specified AS.
in	Without soft, reset the session of the peer to establish active connection.
out	Without soft, reset the session of the local BGP speaker to establish active connection.
soft	Perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration	N/A.

Command mode

Privileged mode.

Usage guidelines

This command is used to reset the sessions of all supported address-families, also including the vrf session in every address-family.

Examples

```
DES-7200# clear bgp ipv4 unicast *
```

Related commands

Command	Description
neighbor soft-reconfiguration inbound	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).
show ip bgp	Show the BGP route entry.

6.1.39 clear bgp ipv4 unicast dampening

Use this command to clear the dampening information and de-suppress the suppressed routes.

clear bgp ipv4 unicast dampening [*address* [*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to clear the BGP route dampening information and de-suppress the suppressed routes. This command can be used to restart the BGP route dampening.

Examples

```
DES-7200# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related commands

Command	Description
show ip bgp dampening dampened-paths	Show the suppressed routing information.
bgp dampening	Enable the route dampening function and set the dampening parameters.

6.1.40 clear bgp ipv4 unicast external

Use this command to reset all EBGP connections.

clear bgp ipv4 unicast external [[**soft**] [**in | out**]]

Parameter description

Parameter	Description
in	Without soft, reset the session of the peer to establish active connection.
out	Without soft, reset the session of the local BGP speaker to establish active connection.
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is used to reset the specified external BGP connection.

Examples

```
DES-7200# clear ip bgp external in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp neighbors	Show the neighbor information.

6.1.41 clear bgp ipv4 unicast flap-statistics

Use this command to clear the unsuppressed routes.

clear bgp ipv4 unicast flap-statistics [*address*[*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command can be used only to clear the statistics of unsuppressed routes. It does not de-suppress the suppressed routes. If you hope to clear all route statistics and de-suppress the suppressed routes, run the **clear ip bgp dampening** command.

Examples

```
DES-7200# clear ip bgp flap-statistics
```

Related commands

Command	Description
bgp dampening	Enable the route dampening function and set the dampening parameters.
show ip bgp	Show the BGP route entry.

6.1.42 clear bgp ipv4 unicast peer-group

Use this command to reset the session with all members in the peer group.

clear bgp ipv4 unicast peer-group *peer-group-name* [[**soft**] [**in** | **out**]]

Parameter description

Parameter	Description
peer-group-name	Name of the peer group.
in	Without soft, reset the session of the peer to establish active connection.
out	Without soft, reset the session of the local BGP speaker to establish active connection.

	soft	Perform soft resetting for all routing information received/sent from/to the specified peer
	soft in	Perform soft resetting for the received routing information.
	soft out	Perform soft resetting for the distributed routing information.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command resets the BGP session with all members in the peer group.

Examples

```
DES-7200# clear ip bgp peer-group my-group in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

6.1.43 clear bgp ipv6 unicast

Use this command to reset the BGP IPv6 unicast address-family.

This command is similar to the **clear bgp ipv4 unicast** except that it is executed in different addess-family.

Parameter description

Parameter	Description
Please refer to the **clear bgp ipv4 unicast** command.	Please refer to the **clear bgp ipv4 unicast** command.

Default configuration Please refer to the **clear bgp ipv4 unicast** command.

Command mode Privileged EXEC mode.

Examples	N/A

Related commands

Command	Description
clear bgp ipv4 unicast	Perform the resetting for the IPv4 unicast address-family.

6.1.44 clear bgp vpnv4 unicast

Use this command to reset the BGP VPNV4 unicast address-family.

This command is similar to the **clear bgp ipv4 unicast** except that it is executed in different addess-family.

Parameter description

Parameter	Description

Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Please refer to the **clear bgp ipv4 unicast** command.
Examples	N/A

Related commands

Command	Description
clear bgp ipv4 unicast	Perform the resetting for the IPv4 unicast address-family.

6.1.45 clear ip bgp

Use this command to reset the BGP session.

clear ip bgp {* |**ipv4 unicast***address* | *as number* } [[**soft**] [**in** | **out**]]

Parameter description

Parameter	Description
*****	Reset all the current BGP sessions.
ipv4	Reset the peer of the specified IPv4 address family.

address	Reset the BGP session with the specified peer.
as number	Reset the sessions with all members in the specified AS.
in	Perform soft resetting for the received routing information.
out	Perform soft resetting for the redistributed routing information.
soft	Perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Note: All connected BGP devices must support the route refresh function to execute this command. This product supports the route refresh function.

At any time, once the routing policy or BGP configuration changes, an effective way must be available to implement the new routing policy or configuration. Traditional measure is to close it and reestablish new BGP connection.

This product supports implementing new routing strategy without the close of the BGP session connection by the configuration of the soft reset for BGP effectively.

For the peer that does not support the route refresh function, you may run the **neighbor soft-reconfiguration inbound** command to keep a copy of original routing information of every specified BGP peer on the local BGP speaker. This will consume some resources.

You can judge whether the BGP peer supports the route refresh function by the **show ip bgp neighbors** command. If it is supported, you need to execute the **neighbor soft-reconfiguration inbound** command when the

inbound routing strategy changes.

Examples

```
DES-7200# clear bgp ipv4 unicast *
```

Related commands

Command	Description
neighbor soft-reconfiguration inbound	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).
show ip bgp	Show the BGP route entry.

6.1.46 clear ip bgp dampening

Use this command to clear the dampening information and de-suppress the suppressed routes.

clear ip bgp [**ipv4 unicast**] **dampening** [*address mask*]

Parameter description

Parameter	Description
ipv4 unicast	IPv4 unicast
address	IP address
mask	Mask

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to clear the BGP route dampening information and de-suppress the suppressed routes. This command can be used to restart the BGP route dampening.

Examples

```
DES-7200# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related commands

Command	Description
show ip bgp dampening dampened-paths	Show the suppressed routing information.

	bgp dampening	Enable the route dampening function and set the dampening parameters.

6.1.47 clear ip bgp external

Use this command to reset all EBGP connections.

clear ip bgp external [**ipv4 unicast**] [[**soft**] [**in | out**]]

Parameter description

Parameter	Description
ipv4 unicast	IPv4 unicast session
in	Without soft, reset the session through which the peer establishes active connection.
out	Without soft, reset the session through which the local BGP speaker establishes active connection.
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is used to reset the specified external BGP connection.

Examples

```
DES-7200# clear ip bgp external in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp neighbors	Show the neighbor information.

6.1.48 clear ip bgp flap-statistics

Use this command to clear the unsuppressed routes.

clear ip bgp flap-statistics [*address*[*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command can be used only to clear the statistics of unsuppressed routes. It does not de-suppress the suppressed routes. If you hope to clear all route statistics and de-suppress the suppressed routes, run the **clear ip bgp dampening** command.

Examples

```
DES-7200# clear ip bgp flap-statistics
```

Related commands

Command	Description
bgp dampening	Enable the route dampening function and set the dampening parameters.
show ip bgp	Show the BGP route entry.

6.1.49 clear ip bgp peer-group

Use this command to reset the session with all members in the peer group.

clear ip bgp peer-group *peer-group-name* [**ipv4 unicast**] [[**soft**] [**in** | **out**]]

Parameter description

Parameter	Description
peer-group-name	Name of the peer group.
ipv4 unicast	ipv4 unicast session
in	Without soft, reset the session through which the peer establishes active connection.
out	Without soft, reset the session through which the local BGP speaker establishes active connection.

soft	Perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command resets the BGP session with all members in the peer group.

Examples

```
DES-7200# clear ip bgp peer-group my-group in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

6.1.50 clear ip bgp table-map

Use this command to clear the application of the table-map route information.

clear ip bgp [**vrf** *vrf-name*] **table-map**

Parameter description

Parameter	Description
vrf-name	vrf name.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is used to clear the application of the table-map route information.

Examples

```
DES-7200# clear ip bgp table-map
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

6.1.51 clear ip bgp vrf

Use this command to reset the BGP sessions of all the members of the VRF.

clear ip bgp vrf *vrf-name* [* *address* }[**soft** [**in** | **out**]]

Parameter description

Parameter	Description
vrf-name	VRF name
*	Reset all the current BGP sessions.
ipv4 unicast	Reset the BGP session of the peer of the IPv4 unicast address family.
address	Reset the BGP session with the specified peer.
in	Without soft, reset the direct session with the specific peer.
out	Without soft, reset the direct session with the BGP speaker.
soft	Perform soft resetting for all routing information received/sent from/to the specified peer.
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command resets the BGP sessions of all the members of the VRF.

Examples	`DES-7200# clear ip bgp vrf my-vrf in`

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

6.1.52 default-information originate

Use this command to distribute the default route. The **no** form of this command is used to disable the distribution of the default route.

default-information originate

[no] default-information originate

Parameter description	N/A
Default configuration	Disabled
Command mode	BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, BGP IPv4 VRF configuration mode.
Usage guidelines	This command is used to control whether the redistributed default route is effective, and this command needs to be configured with the **redistribute** command at the same time. It takes effect only when the routes to be redistributed has the default one. This **default-information originate** command is similar to the **network** command. The difference is that in the process of configuring the former, the **redistribute** command must be configured explicitly to redistribute the default route, only in this case, the redistributed default route are effective. For the later command, the IGP must have the default route.
Examples	`DES-7200(config-router)# default-information originate`

Related

Command	Description

	network	Configure the routes to be advertised.
	redistribute	Redistribute the routes of other protocol.

6.1.53 default-metric

Use this command to set the metric for route redistribution. The **no** form of this command is used to remove the configuration and restore it to the default value.

default-metric number

no default-metric

Parameter description

Parameter	Description
number	Metric number in the range of 1 to 4294967295

Default configuration No metric is set by default.

Command mode BGP configuration mode and various address-family configuration modes

Usage guidelines

This command sets the metric of the routes to be redistributed for integrity.

Note that:

The metric set with the command cannot cover the metric value set with the **redistribute metric** command.

The value is 0 when the default metric applies to the redistributed connected routes.

Examples

```
DES-7200(config-router)# default-metric 45
```

Related commands

Command	Description
redistribute	Redistribute the routes of other protocol.

6.1.54 distance bgp

Use this command to set different management distances for different types of BGP routes. The **no** command is used to restore it to the default.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Parameter description

Parameter	Description
external-distance	Route management distance learned from the EBGP peers in the range: 1 to 255
internal-distance	Route management distance learned from the IBGP peers in the range 1 to 255
local-distance	The management distance of route learned from the peers. However, the optimal one can be learned from the IGP. In general, these routes are indicated by the **Network Backdoor** command. Range: 1 to 255

Default configuration

The parameter defaults are as follows:

external-distance - 20

internal-distance - 200

local-distance - 200

Command mode

BGP configuration mode.

Usage guidelines

It is not recommended to change the management distance of the BGP route. If it is definitely necessary, observe the following points:

1. "*external-distance*" shall have a lower management distance than the other IGP routing protocols (OSPF, RIP, etc.);
2. *internal-distance* and *local-distance* shall have higher management distance than the other IGP routing protocols.

Examples

```
DES-7200(config-router)# distance bgp 20 20 200
```

Related

Command	Description

neighbor soft-reconfiguration inbound	Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).
show ip bgp	Show the BGP route entry.

6.1.55 exit-address-family

Use this command to exit the BGP **address-family** configuration mode.

exit-address-family

Parameter description N/A.

Default configuration N/A.

Command mode BGP **address-family** configuration mode.

Usage guidelines This command can be used to exit from various address-family modes of the BGP to the BGP configuration mode.

Examples

```
DES-7200(config-router-af)#exit-address-family
```

Related commands

Command	Description
address-family ipv4	Enter the **address-family ipv4** configuration mode.

6.1.56 ip as-path access-list

Use this command to specify the regular expression based AS path filtering rule. The **no** command is used to delete the rule.

ip as-path access-list *path-list-num* {**permit** | **deny**}

regular-expression

no ip as-path access-list *path-list-num*

Parameter description

Parameter	Description
path-list-num	Name of the AS path control list based on the regular expression in the range of 1 to 500
permit	Permit the accesses
deny	Deny the accesses
regular-expression	Regular expression Range: 1 to 255 characters.

Default configuration N/A.

Command mode Global configuration mode.

Usage guidelines For the regular expression, see BGP Configuration in the configuration guide.

Examples

```
DES-7200(config-router)# ip as-path access-list 1 deny ^123$
```

Related commands

Command	Description
neighbor filter-list	Apply the AS-path access control list on the specified peer.
neighbor distribute-list	Apply the distribution list on the specified peer.

6.1.57 maximum-prefix

Use this command to limit the maximum number of prefix in the routing database in the address family. Use the **no** form of this command to restore it to the default value.

maximum-prefix *maximum*

no maximum-prefix [*maximum*]

Parameter description

Parameter	Description
maximum	The maximum number of prefix in the routing database in the address family, in the range of 1 to 4294967295.

no	Returns to the default value.

Default configuration

In different addrses families, the default maximum numbers of prefix in the routing database are different:

The default number in the IPv4 VRF, IPv4 Multicast, IPv6 Mulitcast, IPv4 MDT address family is 10000;

The default number in the other address family is 4294967295.

Command mode

BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv4 VRF configuration mode, BGP VPNv4 configuration mode, BGP IPv4 MDT address family mode.

Usage guidelines

In a BGP address family, the routing prefix may be introduced through the redistribute or the neighbor learning, or other VRFs. Once the routing prefix in the BGP address family reaches the maximum number, this address family will enter to the overflow state.

Use the **show bgp** { *addressfamily* | **all** } **summary** command to show the state of routing database.

It is necessary to reconfigure the BGP for state clearing, or use the **clear bgp** { *addressfamily* | **all** } * command to reset the address family.

Note:

When the address family is overflow, it fails to use this command for modification.

Caution:

The maximum-prefix will not filter the routing information generated by the network and aggregate commands.

For the IPv4 unicast routes, even though in the Overflow state, they may still receive the routing prefix in the following conditions:

1. The same routing prefix has existed in the address database.

2. One route that overwrites this prefix (except for the default route) has existed in the address database and the next hop of this route is different from that of the newly received routing prefix.

Examples

The following example shows how to set the maximum number of prefix in the BGP routing database in the ipv4 multicast address family:

```
DES-7200(config)# router bgp 65000

DES-7200(config-router)# address-family ipv4 unicast

DES-7200(config-router-af)# maximum-prefix 65535
```

Related commands

Command	Description
clear bgp { *addressfamily* | **all** } *****	Reset the BGP address-family.
show bgp { *addressfamily* | **all** } **summary**	Show the summary of BGP address-family.

6.1.58 neighbor activate

Use this command to activate the neighbor or peer group in the current address mode. Use the **no** form of the command to restore it tothe default setting.

neighbor {*peer-address* | *peer-group-name*} **activate**

no neighbor {*peer-address* | *peer-group-name*} **activate**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Enabled in address-family IPv4 configuration mode

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode,

Usage guidelines

You need to set this command in other address-family configuration modes for exchaning routes.

Examples

```
DES-7200(config)# router bgp 60
```

```
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 100
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 10.0.0.1 activate
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.59 neighbor advertisement-interval

Use this command to set the time interval to send the BGP route update message. Use the **no** form of the command to restore it to the default setting.

neighbor {*peer-address* | *peer-group-name*} **advertisement-interval** *seconds*

no neighbor {*peer-address* | *peer-group-name*} **advertisement-interval**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
seconds	Time interval to send the route update message in the range of 0 to 600 seconds

Default configuration

IBGP connection: 15seconds

EBGP connection: 30seconds

Command mode

BGP configuration mode.

Usage guidelines

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.0.0.1
advertisement-interval 10
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.

	neighbor remote-as	Configure the BGP peer.

6.1.60 neighbor allowas-in

Use this command to allow the PE to receive the messages of the same AS number as itself. The **no** form restores the setting to the default value.

neighbor {*peer-address* | *peer-group-name*} **allowas-in number**

no neighbor {*peer-address* | *peer-group-name*} **allowas-in**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Number of the AS number duplication in the range of 1 to 10, 3 by default.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

A typical application is spoke-hub mode. Execute this command on the PE to enable it to receive and then send the advertised address prefix. For example, configure two VRFs on the PE. One VRF receives the routes of all PEs and advertises them to the CE; the other VRF receives the routes advertised by the CE and advertises them to all PEs.

This command applies to IBGP peers or EBGP peers.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.1.1.1 remote-as 100
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router-af)# neighbor 10.1.1.1 allowas-in
```

Related

Command	Description

	router bgp	Enable the BGP protocol.
	neighbor remote-as	Configure the BGP peer.

6.1.61 neighbor as-override

Use this command to allow the PE to override the AS number of a site. The **no** form restores the setting to the default value.

neighbor {*peer-address* | *peer-group-name*} **as-override**

no neighbor {*peer-address* | *peer-group-name*} **as-override**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP address-family IPv4 VRF configuration mode.

Usage guidelines

In general, the BGP will not receive the messages of the same AS number as its AS. This command can override the AS number, so that the BGP can receive the messages of the same AS number.

A typical application is in a VPN where two CEs have the same AS number. Usually the CEs cannot receive the messages from each other. Executing this command on a PE will override the AS number of one CE it connects. As a result, the other CE can receive the peer's route messages.

This command applies only to EBGP peers.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.1.1.1 remote-as 100
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router-af)# neighbor 10.1.1.1
as-override
```

Related

Command	Description

router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.62 neighbor default-originate

Use this command to allow the BGP speaker to advertise the default route to the peer (group). The **no** form of the command remove the ocnfiguration.

neighbor {*peer-address* | *peer-group-name*} **default-originate** [**route-map** *map-tag*]

no neighbor {*peer-address* | *peer-group-name*} **default-originate** [**route-map** *map-tag*]

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
map-tag	Name of the route-map of up to 32 characters

Default configuration Disabled.

Command mode BGP configuration mode.

Usage guidelines

This command requires to redistribute the default route only when the default route exists locally.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command. If you set the command for a member in the peer, this command will overwrite the settings on the peer group.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.1.1.1 remote-as 80
DES-7200(config-router)# neighbor 10.1.1.1
default-originate
```

Related

Command	Description

	router bgp	Enable the BGP protocol.
	neighbor remote-as	Configure the BGP peer.

6.1.63 neighbor description

Use this command to set a descriptive sentence for the specified peer (group). The **no** form of the command removes the setting.

neighbor {*peer-address* | *peer-group-name*} **description** *text*

no neighbor {*peer*-address | *peer-group-name*} **description**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
text	Text for describing the peer (group) of up to 80 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command is used to add descriptive characters for the peer (group). This may help remember the features and characteristics of the peer (group).

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.1.1.1 remote-as 80
DES-7200(config-router)# neighbor 10.1.1.1 description
xyz.com
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.64 neighbor distribute-list

Use this ocmmand to configure the ACL based on which the routing policy is implemetned to receiving/transmitting routing information from/to the BGP peer. The **no** form of the command removes the ACL configured.

neighbor {*peer-address* | *peer-group-name*} **distribute-list** *access-list-number* {**in** | **out**}

no neighbor {*peer-address* | *peer-group-name*} **distribute-list** *access-list-number* {**in** |**out**}

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
access-list-number	ACL number
in	Specify the ACL for filtering the incoming routes.
out	Specify the ACL for filtering the outgoing routes.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode .

Usage guidelines

For the **in** rule or **out** rule, this command cannot exist at the same time with the **neighbor prefix-list** command. That is, only one of them takes effect.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command. If you set the **neighbor distribute-list** command for a member in the peer, this command will overwrite the settings on the peer group.

You can set different filtering policies in different address-family configuration modes to control routes.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.1.1.1 remote-as 80
```

```
DES-7200(config-router)# neighbor 10.1.1.1
distribute-list bgp-filter in
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
ip access-list	Create a standard IP ACL or extended IP ACL.

6.1.65 neighbor ebgp-multihop

Use this command to allow the BGP connection established between the EBGP peers that are not directly connected. The **no** form of the command removes the setting.

neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*peer-address* | peer-*group-name*} **ebgp-multihop** [*ttl*]

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
ttl	Maximum hops in the range 1 to 255

Default configuration

The BGP connection is allowed to establish only with the EBGP peer that is directly connected.

If no parameter is used with the "**ebgp-multihop**", the TTL uses 255.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

To prevent routing loop and dampening, non-default routes that can reach the peer must exist between the EBGP peers where the BGP connection must be established via multiple hops.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will

	overwrite the setting for the group.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 remote-as
65100
DES-7200(config-router)# neighbor 10.0.0.1
ebgp-multihop
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.66 neighbor filter-list

When this command is set to specify the BGP peer to receive/transmit routing information, the same route filtering is used. The **no** form of the command cancels the filtering.

neighbor {*peer-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}

no neighbor {*peer-address* | peer-*group-name*} **filter-list** *access-list-number* {**in** | **out**}

Parameter description

Parameter	Description
peer address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
access-list-numbe	ACL number
in	as-path list is applied on the received routing information.
out	as-path list is applied on the distributed routing information.

Default configuration Disabled.

Command mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode .

Usage guidelines	If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If the **neighbor filter-list** command is set for a member of the peer, the setting will overwrite the setting for the group. You can set different filter policies in different address-family configuration modes to control routes.

Examples

```
DES-7200(config)# ip as-path access-list 1 deny _123_
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 65100
DES-7200(config-router)# neighbor 10.0.0.1 filter-list 1 out
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
ip as-path access-list	Create an AS_PATH list.
match as-path	Match the AS_PATH list.

6.1.67 neighbor local-as

Use this command to configure the local AS number for the BGP peer, in this case, this AS could be used as its Remote AS to establish the connection with local router. The **no** form of this command deletes the local AS.

neighbor {*peer-address* | *peer-group-name*} **local-as** *as-number* [**no-prepend** [**replace-as** [**dual-as**]]]

no neighbor {*peer-address* | *peer-group-name*} **local-as**

Parameter description

Parameter	Description
peer address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
as-numbe	Local AS number，in the range of 1 to 65535.
no-prepend	The AS-PATH of the routing information received from the peer dose not append the Local AS. This

	option is disabled by default.
replace-as	The AS-PATH of the routing information sent to the peer uses the Local AS to replace the BGP AS. This option is disabled by default.
dual-as	Use the BGP AS or Local AS to establish the BGP connection with the device. This option is disabled by default.

Default configuration

The Local AS is not configured for the peer. If the Local AS is configured, any options are not configured by default that the peer could only use the Local AS to establish the BGP connection with local device, and adds the Local AS into the AS-PATH of the received routing information, inserts the Local AS to the corresponding AS-PATH before sending the routing information to the peer.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode .

Usage guidelines

The Local AS could be configured on the EBGP peer only, and if the attributes of the peer change, such as the EBGP converts to the IBGP or union EBGP, the Local AS and the corresponding options will be deleted. The Local AS could not be the same with BGP AS and this peer's Remote AS and the union ID (if the union is configured). If you have specified the BGP peer group, all members of this peer group will inherit the settings of this command. You can not set the Local AS for the specified member of the peer group separately.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 remote-as
65100
DES-7200(config-router)# neighbor 10.0.0.1 local-as 23
```

Related

Command	Description

router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.68 neighbor maximum-prefix

Use this command to limit the number of prefixes received from the specified BGP peer. The **no** form of the command removes the limitation configured.

neighbor {*peer-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

no neighbor {*peer*-address | *peer-group-name*} **maximum-prefix** *maximum*

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
Peer-group-name	Name of the peer group of up to 32 characters
maximum	Upeer limit of the number of the received route entries
threshold	Percentage of the maximum when the alarm starts to be generated.
warning-only	Do not determine the BGP connection when the route entries reaches the upeer limit but produce a log entry.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

By default, the BGP connection will be torn down when the received routes exceeds the upeer limit. If you do not hope to tear down the connection, set the "**warning-only**" to control that.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1
maximum-prefix 1000
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.69 neighbor next-hop-self

Use this command to set the next-hop of the route to the local BGP speaker while specifying the routes that the BGP peer redistributes. Use the **no** form of the command to remove the configuration.

neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

no neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command is mostly used in the non-full-mesh-type network, such as the Frame Relay and X.25, where the BGP speakers within the same subnet cannot completely be accessed mutually.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1
next-hop-self
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.70 neighbor next-hop-unchanged

Use this command to unchange the next-hop while sending the routes to the peer(group). Use the **no** form of the command to remove the configuration.

neighbor {*peer-address* | *peer-group-name*} **next-hop-unchanged**

no neighbor {*peer-address* | *peer-group-name*} **next-hop-unchanged**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
next-hop-unchanged	Unchange the next-hop while sending the routes to the peer(group).

Default configuration

By default, the next-hop will be changd while sending the routes to the EBGP peer.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, BGP VPN configuration mode.

Usage guidelines

This command is used to control to unchange the next-hop route that is transmitting between the multi-hop EBGP peer sessions. This command could not be configured on the route reflector. And for the client of the route reflector, if this function is enabled, the neighbor next-hop-self command could not be used to change the next-hop of routes. This function is mainly applied to the cross-domain VPN. In the implementation with the Option C adopted, to reduce the complete connectivity between the PEs of the cross-domain CPN, a route reflector could be set in every autonomous domain to establish the Multihop MP-EBGP connection to implement the VPN route interaction. As the next-hop route is changed while sending routes to the EBGP peer by default, this may cause the PE stations of

other autonomous domains consider the final next-hop of the VPN route to be the route reflector when receiving the VPN route at last, which results in all cross-domains VPN flow going through the reflector. However, usually this is not the optimal forwarding path, and the requirement for the forwarding performance of the RR is higher. To avoid this condition, use the **neighbor next-hop-unchanged** command in the address-family VPNv4 configuration mode to unchange the next-hop of the VPNv4 route that sent to the BGP peer when establishing the cross-domain Multihop MP-EBGP connection on the router reflector.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# address-f00000000amily vpnv4
DES-7200(config-router-af)# neighbor 10.1.1.1
next-hop-unchanged
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.71 neighbor password

When the BGP connection with the BGP peer is established, use this command to enable the TCP MD5 authentication and set the password. The **no** form of the command disables MD5 authentication.

neighbor {*peer-address* | *peer-group-name*} **password** [0 | 7]*string*

no neighbor {*peer-address* | *peer-group-name*} **password**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
0	Display the password with encryption.
7	Display the password without encryption.
string	Password for MD5 authentication in the range of up to 80 characters

Default configuration	Disabled.
Command mode	BGP configuration mod, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.
Usage guidelines	This command will enable the MD5 authentication of the TCP. The BGP peers must have the same password configured; otherwise, the neighbor relationship cannot be established. When this command is set, the local BGP speaker will re-establish the BGP connection with the BGP peer. If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group. A neighbor has only one password, not one for every address family, no matter in which mode it is configured.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# neighbor 10.0.0.1 password DES-7200`

.Related commands

Command	Description
router bgp	Enable the BGP protocol
neighbor remote-as	Configure the BGP peer.

6.1.72 neighbor peer-group (assigning members)

Use this command to configure the specified peer as the member of the BGP peer group. Use the **no** form of this command to delete the specified BGP peer from the peer group.

neighbor *peer-address* **peer-group** *peer-group-name*

no neighbor *peer-address* **peer-group** *peer-group-name*

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32

	characters

Default configuration

No peer exists in the peer group.

Command mode

BGP configuration mode.

Usage guidelines

The members of the peer group can inherit all configurations of the peer.

It is allowed to configure an individual member of the peer group to take the place of the universal configuration for the peer group, but such separate configuration does not contain the configuration information that may affect the output update. In other words, every member in the peer group will always inherit the following configurations of the peer group:

remote-as, update-source, **local-as**,**reconnect-interval** ,**times**, **advertisemet-interval**, **default-originate**, **next-hop-self**, **remove-private-as**, **send-community**, **distribute-list out**, **filter-list out**, **prefix-list out**, **route-map out**, **unsuppress-**map, **route-reflector-client**.

Do not place the neighbors in different address families into the same peer group, and also do not place the IBGP and EBGP neighbors in the same peer group.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor Red-Giant peer-group
DES-7200(config-router)# neighbor 10.0.0.1 peer-group
Red-Giant
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
neighbor peer-group (creating)	Create the BGP peer group.
show ip bgp peer-group	Show the information of the BGP peer.

6.1.73 neighbor peer-group (creating)

Use this command to create the BGP peer group. The **no** form of the command deletes the specified peer group and all its members.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group*-name **peer-group**

Parameter description

Parameter	Description
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

No BGP peer group is created.

Command mode

BGP configuration mode.

Usage guidelines

If multiple BGP peers use the same update policy, those peers can be configured in the same peer group, so as to simplify the configuration and boost operation efficiency.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor Red-Giant peer-group
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
neighbor peer-group (assigning members)	Configure the specified peer as the member of the BGP peer group.
show ip bgp peer-group	Show the information of the BGP peer.

6.1.74 neighbor prefix-list

Use this command to implement the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer. The **no** form of the command removes the prefix-list configured.

neighbor {*peer-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}

no neighbor {*peer-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** |**out**}

Parameter description

Parameter	Description
peer address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
prefix-lis-name	Name of the prefix-list of up to 32 characters
in	Apply the prefix list to the received routes.
out	Apply the prefix list to the redistributed routes.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

For the "**in**" rule or "**out**" rule, this command cannot exist at the same time with the **neighbor distribute-list** command. That is, only one of them takes effect.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If the **neighbor prefix-list in** command is set for a member of the peer, the setting will overwrite the setting for the group.

You can set different filter policies in different address-family configuration modes to control routes.

Examples

```
DES-7200(config)# ip prefix-list bgp-filter deny 10.0.0.1/16
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 prefix-list bgp-filter in
```

Related

Command	Description

commands	**router bgp**	Enable the BGP protocol.
	neighbor remote-as	Configure the BGP peer.
	ip prefix-list	Create the prefix lists.

6.1.75 neighbor remote-as

Use this command to configure the BGP peer (group). The **no** form of the command deletes the configured peer (group).

neighbor {*peer-address* | *peer-group-name*} **remote-as** *as-number*

no neighbor {*peer-address* | *peer-group-name*} **remote-as**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
as-number	BGP peer (group) autonomous system number in the range of 1 to 65535

Default configuration No BGP peer is configured.

Command mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 80
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.

6.1.76 neighbor remove-private-as

Use this command to delete the private AS number recorded in the AS path attribute in the route sent to the specified EBGP peer. Use the **no** form of the command to remove the configuration.

neighbor {*peer-address* | *peer-group-name*} **remove-private-as**

no neighbor {*peer-address* | *peer-group-name*} **remove-private-as**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command takes effect only on the EBGP peers.

If the AS path contains the private AS number that is the AS number of the EBGP peer to be sent, the AS number is not deleted.

Private AS number range: 64512 - 65535

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1
remove-private-as
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.77 neighbor route-map

Use this command to enable route match for the received/sent routes. You can use the **no** form of the command to disable this function.

neighbor {*peer-address*|*peer-group-name* } **route-map** *map-tag* {**in** | **out**}

no neighbor {*peer-address*|*peer-group*-name } **route-map** *map-tag* {**in | out**}

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address

peer-group-name	Name of the peer group of up to 32 characters
map-tag	Name of the match rule
in	Apply the rule to the incoming routes.
out	Apply the rule to the outgoing routes.

Default configuration N/A.

Command mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode and address-family IPv4 VPNv4 cofiguration mode.

Usage guidelines This command can be used to filter the incoming and outgoing routes for different neighbors by using different incoming/outgoing rules. This can reach the results of purifying routes and controlling routes.

You can set different filter policies in different address-family configuration modes to control routes.

Examples

```
DES-7200(config-router)# neighbor ip-address route-map map-tag in
```

Related commands

Command	Description
neighbor soft-reconfiguration inbound	Store the routing information sent from the BGP peer.
show ip bgp	Show the BGP route entry.

6.1.78 neighbor route-reflector-client

Use this command to configure the local device as the route reflector and specifies its client. The **no** form of the command removes the client configured.

neighbor {*ip-address* | *peer-group-name* } **route-reflector-client**

no neighbor {*ip-address* | *peer-group-name* } **route-reflector-client**

Parameter description

Parameter	Description
ip-address	IP address of the peer

	peer-group-name	Name of the peer group of no more than 32 characters

Default configuration	Disabled.
Command mode	BGP configuration mode.
Usage guidelines	By default, all IBGP speakers in the autonomous system must establish neighbor relationship one another. The BGP speaker does not forward the routes learned from an IBGP peer to the other IBGP peers to avoid route loop. This command can be used to set route reflector, so that there is no requirement for all IBGP speakers to establish the full neighboring relationship between each other. This will allow the route reflector to forward the learned IBGP route to the other IBGP peers.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# neighbor 10.0.0.1 route-reflector-client`

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
bgp cluster-id	Configure the cluster ID of the route reflectors.
bgp client-to-client reflection	Cancel the route reflection between clients

6.1.79 neighbor send-community

Use this command to transmit the community attributes to the specified BGP neighbor. Use the **no** form of the command to disable this function.

neighbor {*peer-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

no neighbor {*peer-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

Parameter description

Parameter	Description
peer-addres	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
both	Transmit both standard and extended communities.
standard	Transmit the standard community only.
extended	Transmit the extended community only.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode and address-family IPv4 VPNv4 configuration mode.

Usage guidelines

This command transmits the community to the neighbor or neighbor group.

Examples

```
DES-7200(config-router)# neighbor 10.1.1.1
send-community both
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
ip community-list	Create the community list.

6.1.80 neighbor send-label

Use this command to specify to carry the MPLS label of the route whren sending the route to the a neighbor. Use the **no** form of the command to disable this function.

neighbor {*peer-address* | *peer-group-name*} **send-label**

no neighbor {*peer-address* | *peer-group-name*} **send-label**

Parameter description

Parameter	Description
peer-addres	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode and address-family VPNv4 configuration mode.

Usage guidelines

Use this command to allow the BGP sending the routes with MPLS label requiring two ends of the peer should be configured this command. The configuration of this command takes effect only after restarting the neighbor. This command is configured in the BGP configuration mode and takes effect on the ipv4 unicast address-family only by default. For the AS border routers, only when this command is configured, the MPLS label forwarding on the AS border could be implemented.

Examples

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# neighbor 192.168.0.1 remote-as 101
DES-7200(config-router)# neighbor 192.168.0.1 send-label
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.81 neighbor shutdown

Use this command to disconenct the BGP connection established with the specified BGP peer. The **no** form of the command reconnects the BGP peer (group).

neighbor {*peer-address* | *peer-group-name*} **shutdown**

no neighbor {*peer-address* | *peer-group-name*} **shutdown**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command is used to disconnect the valid connection established with the specified peer (group), and delete all associated routing information. However, this command still keeps the configuration information of that specified peer (group).

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.0.0.1 shutdown
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
show ip bgp summary	Show the BGP connection status.

6.1.82 neighbor soft-reconfiguration inbound

Use this command to sotre the routing information sent from the BGP peer. Use the **no** form of the command to disable them.

neighbor {*peer-address* | *peer-group-name*} **soft-reconfiguration inbound**

no neighbor {*peer-address* | *peer-group-name*} **soft-reconfiguration inbound**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command restarts the BGP session, and keeps the unchanged routing information sent from the BGP peer (group).

Executing this command will consume more memories. If both parties support the route refresh function, this command becomes unnecessary. You may run the **show ip bgp neighbors** command to judge whether the peer can support the route refresh function.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1
soft-reconfiguration inbound
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
show ip bgp neighbors	Show the information of the BGP peer.
clear ip bgp	Reset the BGP peer session.

6.1.83 neighbor soo

Use this command to set the SOO value of the neighbor. Use the **no** form of the command to remove the configuration.

neighbor {*peer-address* | *peer-group-name*} **soo** *soo-value*

no neighbor {*peer-address* | *peer-group-name*} **soo** *soo-value*

Parameter description

Parameter	Description
peer-addres	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
soo-value	SOO value. There are two forms of SOO value: as_number:nn: as_number is the public AS number and nn is defined by yourself. ip_address:nn: IP address must be global and nnis defined by yourself.

Default configuration

Disabled.

Command mode

Address-family IPv4 VRF configuration mode

Usage guidelines

In the CE dual-home mode, execute this command to prevent the routes that a CE sends to the PEs from being sent back to the CE.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 100
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router)# neighbor 10.0.0.1 soo 100:100
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
timers bgp	Configure the keepalive and holetime values globally.

6.1.84 neighbor timers

In specifying the BGP peer to establish the BGP connection, use this command to set the *keepalive* and *holdtime* time values used for establishing the BGP connection. Use the **no** form of the command to restore it to the default setting.

neighbor [*peer-address* | *peer-group-name*] **timers** *keepalive holdtime*

no neighbor [*peer-address* | *peer-group-name*] **timers**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
keepalive	Time interval to send the KEEPALIVE message to the BGP peer. Range: 0-65535 seconds.
holdtime	Time interval to consider the BGP peer alive. Range: 0-65535 seconds.

Default configuration

keepalive: 60 seconds

holdtime: 180 seconds.

minimum-holdtime: 0 second

Command mode

BGP configuration mode.

Usage guidelines

A reasonable *keepalive* value cannot be greater than one-third of the holdtime value.

If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 80 240
```

Related

Command	Description

router bgp	Enable the BGP protocol.
timers bgp	Set the *keepalive* and *holdtime* values globally.

6.1.85 neighbor unsuppress-map

Use this command to selectively advertise the routing information that has been suppressed with the **aggregate-address** command. Use the **no** form of the command to restore it to the default setting.

neighbor {*peer-address* | *peer-group-name*} **unsuppress-map** *map-tag*

no neighbor {*peer-address* | *peer-group-name*} **unsuppress-map** *map-tag*

Parameter description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
map-tag	Name of the route-map of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command advertises the specified routes that has been suppressed.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1
unsuppress-map unspress-route
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

aggregate-address	Configure the aggregate address.
route-map	Configuring route-map

6.1.86 neighbor update-source

In specifying the BGP peer to establish the BGP connection, use this command to set the network interface used for establishing the BGP connection. The **no** form of the command automatically matches the optimal local interface.

neighbor {*peer-address* | *peer-group-name*} **update-source** *interface-type interface-index*

no neighbor {*peer-address* | *peer-group*-name} **update-source** *interface-type interface-index*

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
interface-type	Interface type
interface-index	Interface index

Default configuration

Use the optimal local interface as the output interface.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command enables using the loopback interface to establish the BGP connection with the BGP peer.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

If the connection is initiated by the opposite, it does not check which interface is used to establish the TCP connection.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1
update-source lookback 1
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.87 neighbor version

Use this command to show the number of the BGP protocol version used by the specific BGP neighbor. The **no** form of the command uses the default version number.

neighbor {*ip-address*|*peer-group-name*} **version** *number*

no neighbor {*ip-address*|*peer-group-name*} **version** *number*

Parameter description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Version Number. Now only version 4 is supported.

Default configuration The default version number is 4.

Command mode BGP configuration mode.

Usage guidelines When the command is used, the BGP will lose the version negotiation function.

Examples

```
DES-7200(config-router)# neighbor 10.1.1.1 version 4
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.88 neighbor weight

Use this command to set the weight for the specific neighbor. The **no** form of the command removes the setting.

neighbor {*ip-address*|*peer-group-name*} **weight** *number*

no neighbor {*ip-address*|*peer-group-name*} **weight** *number*

Parameter description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Weight in the range of 0 to 65535.

Default configuration

No weight is configured for the specific neighbor by default. In this case, the learned neighbor weight is 0 and the locally generated weight is 32768 initially.

Command mode

BGP configuration mode.

Usage guidelines

When the command is used, the routes from the neighbor use this value as the initial weight value. The higher the weight, the higher the priority is.

Executing the **set weight** command in the route map of the neighbor will overwrite this value.

Examples

```
DES-7200(config-router)# neighbor 10.1.1.1 weight 73
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

6.1.89 network(BGP)

Use this command to configure the network information to be advertised by the local BGP speaker. The **no** form of the command deletes the configured network information.

network *network-number* **mask** *mask* [**route-map** *map-tag*] [**backdoor**]

no network *network-number* **mask** *mask* [**route-map**] [**backdoor**]

Parameter description

Parameter	Description
network-number	Network number

mask	Subnet mask
map-tag	Name of the route-map of up to 32 characters
backdoor	The route is a backdoor route.

Default configuration

The network information is not specified.

Command mode

BGP configuration mode.

Usage guidelines

This command allows injecting the IGP route into the BGP routing table. The network information advertised can be direct route, static route and dynamic route.

The "**route-map**" can be used to modify the network information.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# network 10.0.0.1 mask
255.255.0.0
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
redistribute	Configure the route redistribution.
Network synchronization	Enalbe network synchronization.

6.1.90 network synchronization

Use this command to advertise the network information after the local BGP speaker is synchronized with the local device. The **no** form of the command directly advertises the network information.

network synchronization

no network synchronization

Parameter description

N/A.

Default configuration

Enabled.

Command mode	BGP configuration mode.
Usage guidelines	This command is used to modify the behavior of the network during the process of advertisement. It is not recommended to turn off this switch lest route black hole is caused.
Examples	`DES-7200(config)# router bgp 65000` `DES-7200(config-router)# network synchronization`

Related commands

Command	Description
router bgp	Enable the BGP protocol.
redistribute	Configure the route redistribution.
network(BGP)	Configure the route to be distributed.

6.1.91 overflow memory-lack

Use this command to allow the BGP to enter the OVERFLOW state when the memory lacks. Use the **no** form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

Parameter description

Parameter	Description
no	Disallow the BGP to enter the OVERFLOW state when the memory lacks.

Default configuration	Allow the BGP to enter the OVERFLOW state when the memory lacks.
Command mode	BGP configuration mode.
Usage guidelines	In the BGP OVERFLOW state, the newly-learned routes are discarded, which prevents the memory from being increased. With this function enabled, if the BGP address family is in

	the OVERFLOW state, the newly-learned routes will be discarded, which may results in the loop in the network. To prevent that from happening and reduce the propability, BGP generates a default route directing to the NULL interface, and the default route will always exist in the OVERFLOW state. Use the **clear bgp** {addressfamily**|all**} * command to reset the BGP and clear the OVERFLOW state in the BGP address family. Use the no option to disallow the BGP to enter the OVERFLOW state when the memory lacks, which is possible to lead to the continuous exhausion of the memory resources. When the meory has been exhausted to a certain degree, BGP will break down all neighbors and delete all learned routes.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# no memory-lack overflow
```

Related commands

Command	Description
clear bgp { *addressfamily*|**all** } *	Reset the BGP address family.
show bgp { *addressfamily*|**all** } **summary**	Show the summary of the BGP address family.

6.1.92 redistribute

Use this is to redistribute routes between the other routing protocol and the BGP. The **no** form of the command disables the function.

redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

no redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

Parameter description

Parameter	Description
protocol-type	The source protocol types for redistributing routes, including connected, static, RIP.
route-map *map-tag*	Specify the route map. No route map is associated with by default.
metric	Set the default metric of the routes to

	metric-value	be redistributed, null by default.

Default configuration	Disabled.
Command mode	BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.
Usage guidelines	When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols. Note that when you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured. The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Examples	`DES-7200(config-router)# redistribute static route-map static-rmap`
	`DES-7200(config-router)# no redistribute static route-map static-rmap`
	`DES-7200(config-router)# no redistribute static`

Related commands	Command	Description
	show ip protocol	Show the protocol configuration.

6.1.93 redistribute ospf

Use this is to redistribute routes between the OSPF and the BGP. The **no** form of the command disables the function.

redistribute *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [1 | 2] **nssa-external** [1 | 2]]

no redistribute *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [1 | 2] **nssa-external** [1 | 2]]

Parameter description

Parameter	Description
process-id	OSPF process ID to be redistributed
route-map *map-tag*	Specify the route map. No route map is associated with by default.
metric *metric-value*	Set the default metric of the routes to be redistributed, null by default.
match	Match the sub type of OSPF routes.
internal	Match the internal OSPF routes, the default configuration.
external [1 | 2]	Match the external OSPF rotues. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.
nssa- external [1 | 2]	Match the NSSA-external type of OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

Note that when you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.

The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Examples

```
DES-7200(config-router)# redistribute ospf 2 route-map static-rmap
```

```
DES-7200(config-router)# no redistribute ospf 4 match
external rotue-map ospf-rmap
DES-7200(config-router)# no redistribute ospf 78
```

Related commands

Command	Description
show ip protocol	Show the protocol configuration.

6.1.94 redistribute isis

Use this is to redistribute routes between the ISIS and the BGP. The **no** form of the command disables the function.

redistribute isis [*isis-tag*] [**route-map** *map-tag*] [**metric** *metric-value*] [**level-1** | **level-1-2** | **level-2**]

no redistribute isis [*isis-tag*] [**route-map** *map-tag*] [**metric** *metric-value*] [**level-1** | **level-1-2** | **level-2**]

Parameter description

Parameter	Description
isis-tag	(Optional)ISIS process ID to be redistributed
route-map *map-tag*	Specify the route map. No route map is associated with by default.
metric *metric-value*	Set the default metric of the routes to be redistributed, null by default.
level-1	Redistribute level-1 ISIS routes.
level-1-2	Redistribute level-1 and level-2 ISIS routes.
level-2	Redistribute level-2 ISIS routes.

Default configuration Disabled.

Command mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode.

Usage guidelines When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute the

protocols. This is applicable to all IP routing protocols.

Note that when you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.

The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Examples

```
DES-7200(config-router)# redistribute isis route-map static-rmap
DES-7200(config-router)# no redistribute isis test route-map isis-rmap
DES-7200(config-router)# no redistribute isis
```

Related commands

Command	Description
show ip protocol	Show the protocol configuration.

6.1.95 router bgp

Use this command to enable the BGP protocol, configure the local autonomous system number and enter the BGP protocol configuration mode. The **no** form of the command disables the BGP protocol.

router bgp *as-number*

no router bgp *as-number*

Parameter description

Parameter	Description
as-number	AS number in the range 1 to 65535

Default configuration Disabled.

Command mode Global configuration mode.

Usage guidelines This command is used to start the BGP protocol.

Examples

```
DES-7200(config)# router bgp 65000
```

Related commands

Command	Description
ip routing	Enable IP routing.
bgp router-id	Set the ID of the device running the BGP protocol
network	Set the network information to be advertised by the local BGP speaker.

6.1.96 synchronization

Use this command to enable the synchronization mechanism of the BGP and IGP routing information. The **no** form of the command disables the synchronization mechanism of the BGP and IGP routing information.

synchronization

no synchronization

Parameter description

N/A.

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

The synchronization between BGP and IGP aims to prevent the possible route black hole.

In any of the two cases below, you may cancel the synchronization mechanism to ensure fast convergence of routing information.

1. There is no the route information which pass through this AS (In general, this AS is an end AS).
2. All devices within this AS operate the BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# synchronization
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.

6.1.97 table-map

Use this command to control the route information distributed to the kernel table.

table-map *route-map-name*

no table-map

Parameter description

Parameter	Description
route-map-name	Name of the route-map

Default configuration N/A

Command mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines BGP uses the table-map to control the information that distributed to the kernel routing table. The table-map is used to modify the attributes of that route information, and it only takes effect on the IPv4 address-family.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# table-map bgp_tm
```

Related commands

Command	Description
route-map	Configure the route-map

6.1.98 timers bgp

Use this command to adjust the BGP network timer. The **no** form of the command restores the default value.

timers bgp *keepalive holetime*

Parameter description

Parameter	Description
keepalive	Time interval to send the keepalive message to the BGP peer. Range: 0-65535 seconds.
holdtime	Time interval to consider the BGP peer alive. Range: 0-65535 seconds.

Default configuration

keepalive: 60 seconds

holdtime: 180 seconds

minum-holdtime: 0 second

Command mode

BGP configuration mode.

Usage guidelines

A reasonable *keepalive* value cannot be greater than one-third of the holdtime value.

If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# timers bgp 80 240
```

Related commands

Command	Description
neighbor timers	Set the *keepalive* and *holdtime* values on the basis of neighbors.

6.2 Showing Related Command

6.2.1 show ip bgp

Use this command to show the route information of BGP.

show ip bgp [{*network* | *network-mask*}] [**longer-prefixes**]

Parameter description

Parameter	Description
network	Showing the specific routing information in the routing table
network-mask	Show the routing information included in the specified network.
longer-prefixes	Show the routing information of a route, including the more specific routes included in it.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines Use this command to view the route information of BGP.

Examples

```
DES-7200# show ip bgp
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status   Network       Next Hop   Metric  LocPrf   Path
------ --------  -------   --------  --------
-------------
*>  211.21.21.0/24  110.110.110.10  0     1000   200 300
*>  211.21.23.0/24  110.110.110.10  0     1000   200 300
*>  211.21.25.0/24  110.110.110.10  0     1000   300
*>  211.21.26.0/24  110.110.110.10  0     1000   300
*>  211.21.27.0/24  110.110.110.10  0     1000   200
```

6.2.2 show bgp all

Use this command to show all the address-families information of BGP route. The use of this command is consistent with other BGP's show commands.

Show the parameters of the route information.

show bgp all [**community** | **filter-list** | **community-list** | **dampening** {**flap-statistics** | **dampened-paths**} | **regexp** | **quote-regexp** | **neighbors** {**received-routes** | **routes** | **advertised-routes**}]

Show the route dampening parameter

show bgp all dampening parameters

Show the related information of the neighbors

show bgp all neighbors

show bgp all summary

Show the path information

show bgp all paths

Parameter description

Parameter	Description
Please refer to the detaied description of **show bgp ipv4 unicast** command.	Please refer to the detaied description of **show bgp ipv4 unicast** command.

Default configuration

Please refer to the detaied description of **show bgp ipv4 unicast** command.

Command mode

Privileged EXEC mode.

Usage guidelines

Please refer to the detaied description of **show bgp ipv4 unicast** command..

Related commands

Command	Description
show bgp ipv4 unicast	Show the IPv4 unicast route information of BGP

6.2.3 show bgp ipv4 mdt

Use this command to show the ipv4 mdt routing or neighbor information of all vrfs or rds.

show bgp ipv4 mdt all [*network* | **neighbor** [*address*] | **summary**]

show bgp ipv4 mdt rd *rd_value* [*network*]

Parameter description

Parameter	Description
network	Specified network address
neighbor	Show the neighbor information of the route.
address	Show the specific neighbor information.

summary	Show the main information of the route.
rd_value	RD value, such as 100:1 or 202.118.239.165:1

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to show all ipv4 mdt routing information of all vrf or rd.

Examples

```
DES-7200# show bgp ipv4 mdt all
BGP table version is 0, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Route Distinguisher: 78:90 (Default for VRF this)
   Network          Next Hop            Metric     LocPrf
Path
*>  202.210.10.0       177.36.51.3                   0
10 i
*>i208.208.1.0     192.168.195.183        0        100
i
*>i208.208.2.0     192.168.195.183        0        100
i
*>  211.158.0.0        0.0.0.0                       0
i
*>i211.158.1.0     192.168.195.183        0        100
i
*>  212.210.0.0        0.0.0.0                       0
i
*>  212.210.1.0        0.0.0.0                       0
i
```

```
Total number of prefixes 7

DES-7200# show bgp ipv4 mdt all summary

BGP router identifier 192.168.183.1, local AS number 23

BGP table version is 1

2 BGP AS-PATH entries

1 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd

177.36.51.2     4    10       0       0        0    0    0
never Active

177.36.51.3     4    10      85      87        1    0    0
01:12:25       5

Total number of neighbors 2
```

Related commands	Command	Description
	-	-

6.2.4 show bgp ipv4 unicast

Use this command to show the IPv4 unicast route information of BGP.

show bgp ipv4 unicast [*network* [*network-mask*]]

show bgp ipv4 unicast community *community-number* [**exact-match**]

show bgp ipv4 unicast community-list *community-name* [**exact-match**]

show bgp ipv4 unicast dampening dampened-paths

show bgp ipv4 unicast dampening flap-statistics

show bgp ipv4 unicast filter-list *path-list-number*

show bgp ipv4 unicast inconsistent-as

show bgp ipv4 unicast prefix-list *ip-prefix-list-name*

show bgp ipv4 unicast quote-regexp *regexp*

show bgp ipv4 unicast regexp *regexp*

show bgp ipv4 unicast route-map *map-tag*

show bgp ipv4 unicast neighbors *neighbor-address* [**received-routes** | **routes** | **advertised-routes**]

show bgp ipv4 unicast cidr-only

show bgp ipv4 unicast labels

Parameter description

Parameter	Description
network	Showing the specific routing information in the routing table
network-mask	Show the routing information included in the specified network.
community *community-number*	Show the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet,no-export, local-as, no-advertise.
community-list *community-name*	Show the BGP routing information matching the specifed community-list.
exact-match	Routing information exactly matching the community value or community-list.
dampening dampened-paths	Show the restained routing information.
dampening flap-statistics	Show the routing dampening statistics.
filter-list *path-list-number*	Show the routing information matching the filter-list.
inconsistent-as	Show the routing information of the inconsistent source AS.
prefix-list *ip-prefix-list-name*	Show the routing information matching the specified prefix-list.
quote-regexp *regexp*	Show the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
route-map *map-tag*	Show the routing information matching the specified route-map filtering condition.
neighbors *neighbor-address* **received-routes**	Show all routing information received from the specified peer (including the accepted and refused route).

neighbors *neighbor-address* **routes**	Show all the routing information received from the peer and accepted.
neighbors *neighbor-address* **advertised-routes**	Show all the routing information sent to the specified peer.
cidr-only	Show the routing information without the category.
labels	Show the BGP-learnt and BGP-sent routes with the MPLS label.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to view the IPv4 unicast route information of BGP. You can filter the information with the specifed parameter to show the matching route information.

Examples

```
DES-7200# show bgp ipv4 unicast
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop           Metric     LocPrf
Path
*>i44.0.0.0        192.168.195.183         0        100
i
*>i64.12.0.0/16     192.168.195.183         0        100
i
*>i172.16.0.0/24    192.168.195.183         0
100     i
*>i202.201.0.0      192.168.195.183         0        100
i
*>i202.201.1.0      192.168.195.183         0        100
i
*>i202.201.2.0      192.168.195.183         0        100
i
*>i202.201.3.0      192.168.195.183         0        100
i
```

```
*>i202.201.18.0    192.168.195.183        0       100
i
Total number of prefixes 8
DES-7200# show bgp ipv4 unicast community 11:2222
111:12345
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal,
           S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop          Metric     LocPrf
Path
*>i202.201.0.0     192.168.195.183        0       100
i
*>i202.201.1.0     192.168.195.183        0       100
i
*>i202.201.2.0     192.168.195.183        0       100
i
*>i202.201.3.0     192.168.195.183        0       100
i
Total number of prefixes 4
DES-7200(config)# ip as-path access-list 5 permit .*
DES-7200# show bgp ipv4 unicast filter-list 5
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal,
           S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop          Metric     LocPrf
Path
*>192.168.88.0     0.0.0.0             32768 ?
Total number of prefixes 1
DES-7200# show ip bgp cidr-only
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal,
           S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop          Metric     LocPrf
Path
*>i64.12.0.0/16    192.168.195.183        0       100
i
*>i172.16.0.0/24   192.168.195.183        0
100     i
Total number of prefixes 2
DES-7200# show bgp ipv4 unicast labels
Network         Next Hop        In Label/Out Label
1.1.1.1/32      192.167.1.1     17/18
1.1.1.2/32      192.167.1.1     nolabel/19
```

Table Fields in the output information

Field	Description
Network	Route prefix
Nexthop	Nexthop IP address of the route
In label	Label assigned by this router (if existing.)
Out label	Lable learnt from the nexthop router.(if existing)

Related commands

Command	Description
show ip bgp	Show the IPv4 unicast route information of BGP.

6.2.5 show bgp ipv4 unicast dampening parameters

Use this command to show the IPv4 unicast route dampening parameters configured for the BGP.

show bgp ipv4 unicast dampening parameters

Parameter description

N/A.

Default configuration

N/A.

Command mode

Privileged EXEC mode

Usage guidelines

This command is used to show the IPv4 unicast route dampening parameters configured for the BGP.

Examples

```
DES-7200(config-router)# bgp dampening 25 10000 10000 200
DES-7200# show bgp ipv4 unicast dampening parameters
dampening 25 10000 10000 200
Dampening Control Block(s):
Reachability Half-Life time    : 25 min
Reuse penalty                  : 10000
Suppress penalty               : 10000
Max suppress time              : 200 min
```

```
Max penalty (ceil)              : 29800000
Min penalty (floor)             : 5000
```

6.2.6 show bgp ipv4 unicast neighbors

Use this command to show the related information of BGP IPv4 unicast neighbor.

show bgp ipv4 unicast neighbors *neighbor-address*

Parameter description

Parameter	Description
neighbor-address	IP address of the neighbor

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to view the information of the connection with BGP IPv4 unicast neighbor.

Examples

```
DES-7200# show bgp ipv4 unicast neighbors
BGP neighbor is 192.168.195.183, remote AS 23, local AS
23, internal link
  BGP version 4, remote router ID 44.0.0.1
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval
is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Graceful restart: advertised and received
Remote Restart timer is 120 seconds
  Received 14 messages, 0 notifications, 0 in queue
    open message:1 update message:4 keepalive message:9
    refresh message:0 dynamic cap:0 notifications:0
  Sent 12 messages, 0 notifications, 0 in queue
    open message:1 update message:3 keepalive message:8
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Inbound soft reconfiguration allowed
  8 accepted prefixes
  0 announced prefixes
 Connections established 2; dropped 1
```

```
Local host: 192.168.195.239, Local port: 1074
Foreign host: 192.168.195.183, Foreign port: 179
Nexthop: 192.168.195.239
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:06:43, due to BGP Notification sent
Notification Error Message: (Cease/Unspecified Error
Subcode)
Using BFD to detect fast fallover
```

Related commands	

6.2.7 show bgp ipv4 unicast paths

Use this command to show the path information of the IPv4 unicast in the route database.

show bgp ipv4 unicast paths

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the path information in the route database.
Examples	DES-7200# **show bgp ipv4 unicast paths** Address Refcnt Path [0x1d7806a0:0] (67) [0x1d7389a0:13] (20) 10

6.2.8 show bgp ipv4 unicast summary

Use this command to show the related information of BGP IPv4 unicast.

show bgp ipv4 unicast summary

Parameter description	N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the related information of BGP IPv4 unicast.

Examples

```
DES-7200 # show bgp ipv4 unicast summary
BGP router identifier 192.168.183.1, local AS number 23
BGP table version is 2
2 BGP AS-PATH entries
1 BGP community entries
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
192.168.195.79  4    24      0       0       0    0    0
never Active
192.168.195.183 4    23     17      15       1    0    0
00:09:04       8
Total number of neighbors 2
```

Related commands

Command	Description
router bgp	Enable the BGP protocol

6.2.9 show bgp ipv6 unicast

Use this command to show the IPv6 unicast routing information of BGP.

show bgp ipv6 unicast [*IPv6-Prefix*]

show bgp ipv6 unicast community *community-number* [**exact-match**]

show bgp ipv6 unicast community-list *community-name* [**exact-match**]

show bgp ipv6 unicast dampening dampened-paths

show bgp ipv6 unicast dampening flap-statistics

show bgp ipv6 unicast filter-list *path-list-number*

show bgp ipv6 unicast inconsistent-as

show bgp ipv6 unicast prefix-list *ipv6-prefix-list-name*

show bgp ipv6 unicast quote-regexp *regexp*

show bgp ipv6 unicast regexp *regexp*

show bgp ipv6 unicast route-map *map-tag*

show bgp ipv6 unicast neighbors *neighbor-address* [**received-routes** | **routes** | **advertised-routes**]

Parameter description

Parameter	Description
IPv6-prefix	Show the IPv6 routing information included in the specified network. The input format of the routing information prefix is X:X:X:X::X/<0-128>.
community *community-number*	Show the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet,no-export, local-as, no-advertise.
community-list *community-name*	Show the BGP routing information matching the specifed community-list.
exact-match	Routing information exactly matching the community value or community-list.
dampening dampened-paths	Show the restained routing information.
dampening flap-statistics	Show the routing dampening statistics.
filter-list *path-list-number*	Show the routing information matching the filter-list.
inconsistent-as	Show the routing information of the inconsistent source AS.
quote-regexp *regexp*	Show the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
route-map *map-tag*	Show the routing information matching the specified route-map filtering condition.
neighbors *neighbor-address* **received-routes**	Show all routing information received from the specified peer (including the accepted and refused route).

	neighbors *neighbor-address* **routes**	Show all the routing information received from the peer and accepted.
	neighbors *neighbor-address* **advertised-routes**	Show all the routing information sent to the specified peer.

Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to view the IPv6 unicast route information of BGP. You can filter the information with the specifed parameter to show the matching route information. The function and use of this command is similar to the **show bgp ipv4 unicast** command, please refer to it.
Examples	N/A

Related commands

Command	Description
show bgp ipv4 unicast	Show the IPv4 unicast route information of BGP.

6.2.10 show bgp ipv6 unicast dampening parameters

Use this command to show the IPv6 unicast route dampening parameters configured for the BGP.

show bgp ipv6 unicast dampening parameters

Parameter description	N/A.
Default configuration	N/A.

Command mode	Privileged EXEC mode
Usage guidelines	This command is used to show the IPv6 unicast route dampening parameters configured for the BGP. The function and use of this command are similar to the **show bgp ipv4 unicast dampening parameters** command, please refer to it.
Examples	N/A.

Related commands

Command	Description
show bgp ipv4 unicast dampening parameters	Show the IPv4 unicast route dampening parameters configured for the BGP.

6.2.11 show bgp ipv6 unicast neighbors

Use this command to show the related information of BGP IPv6 unicast neighbor.

show bgp ipv6 unicast neighbors *neighbor-address*

Parameter description

Parameter	Description
neighbor-address	IP address of the neighbor

Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the information of the connection with BGP IPv6 unicast neighbor. The function and use of this command are similar to the **show bgp ipv4 unicast neighbors** *neighbor-address* command, please refer to it.
Examples	N/A

Related

Command	Description

commands	**show bgp ipv4 unicast neighbors** *neighbor-address*	Show the related information of BGP IPv4 unicast neighbor.

6.2.12 show bgp ipv6 unicast paths

Use this command to show the path information of the IPv6 unicast in the route database.

show bgp ipv6 unicast paths

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the path information in the route database.
Examples	DES-7200# **show bgp ipv6 unicast paths** Address Refcnt Path [0x1d7806a0:0] (67) [0x1d7389a0:13] (20) 10

Related commands	Command	Description
	show bgp ipv4 unicast paths	show the path information of the IPv4 unicast in the route database.

6.2.13 show bgp ipv6 unicast summary

Use this command to show the related information of BGP IPv6 unicast.

show bgp ipv6 unicast summary

Parameter description	N/A.
Command mode	Privileged EXEC mode.

Usage guidelines	This command is used to show the related information of BGP IPv6 unicast. The function and use of this command are similar to the **show bgp ipv4 unicast summary** command, please refer to it.
Examples	N/A

Related commands

Command	Description
router bgp	Enable the BGP protocol
show bgp ipv4 unicast summary	show the related information of BGP IPv4 unicast.

6.2.14 show bgp vpnv4 unicast

Use this command to show the VPN or neighbor information of all the VRFs or RDs.

show bgp vpnv4 unicast all [*network* | **neighbor** [| *address*] | **summary** | **labels**]

show bgp vpnv4 unicast vrf *vrf_name* [*network* | **summary** | **labels**]

show bgp vpnv4 unicast rd *rd_value* [*network* | **summary**| **lables**]

Parameter description

Parameter	Description
network	Network IP address
neighbor	Show neighbor information.
labels	Show the label information of routes.
vrf_name	VRF name
rd_value	RD value, for example, 100:1 or 202.118.239.165:1
summary	Show the route summary information.

Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the VPN information of all VRFs or RDs.

Examples

```
DES-7200# show bgp vpnv4 unicast all
BGP table version is 0, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid,
```

```
> best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Route Distinguisher: 78:90 (Default for VRF this)
   Network         Next Hop           Metric     LocPrf
Path
*> 202.210.10.0    177.36.51.3             0
10 i
*>i208.208.1.0     192.168.195.183         0        100
i
*>i208.208.2.0     192.168.195.183         0        100
i
*> 211.158.0.0     0.0.0.0                 0
i
*>i211.158.1.0     192.168.195.183         0        100
i
*> 212.210.0.0     0.0.0.0                 0
i
*> 212.210.1.0     0.0.0.0                 0
i
Total number of prefixes 7
DES-7200# show bgp vpnv4 unicast vrf this summary
BGP router identifier 192.168.183.1, local AS number 23
BGP VRF this Route Distinguisher: 78:90
BGP table version is 1
2 BGP AS-PATH entries
1 BGP community entries
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
177.36.51.2     4    10      0       0       0    0    0
never Active
177.36.51.3     4    10     85      87       1    0    0
01:12:25        5
Total number of neighbors 2
```

6.2.15 show ip as-path-access-list

Use this command to show the related information of the AS path ACL.

show ip as-path-access-list [*num*]

Parameter description

Parameter	Description
num	AS path ACL number

Default configuration N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the **as-path-access-list** information.
Examples	DES-7200# **show ip as-path-access-list** AS path access list 30 permit ^30s

7 PBR Commands

7.1 Configuration Related Commands

7.1.1 ip local policy route-map

Use this command to enable the policy-based routing for the packets sent locally. The **no** format of this command disables the function.

ip local policy route-map *route-map*

no ip local policy route-map

Parameter description

Parameter	Description
route-map	Name of the route map

Default Disabled.

Command mode Global configuration mode.

Usage guidelines

This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets sent received by the local is free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

Examples The following examples shows how to send the packets with the source addresss 192.168.217.10 to 192.168.4.7.

Example1: define the ACL matched the IP packet

```
DES-7200(config)#access-list 1 permit 192.168.217.10
```

Example2: define the route map

```
DES-7200(config)#route-map lab1 permit 10
DES-7200(config-route-map)#match ip address 1
DES-7200(config-route-map)#set ip next-hop 196.168.4.7
DES-7200(config-route-map)#exit
```

Example3: apply the policy-based routing on the local interface:

```
DES-7200(config)#ip local policy route-map lab1
```

Related commands

Command	Description
access-list	Define the access list rule.
route-map	Define the route map.
set vrf	Define the VRF instance of the policy-based IP packet.
set ip next-hop	Define the next hop of the policy-based routing.
set ip default next-hop	Define the default next hop of the policy-based routing.
set ip tos	Set the TOS in the head of the IP packet.
set ip dscp	Set the DSCP of the IP packet.
set ip precedence	Set the priority level in the head of the IP packet.
match ip address	Set the IP address.

7.1.2 ip policy

Use this command to set the policy applied for the **set ip nexthop** command in the global configuration mode. The **no** form restores the forwarding mode of policy-based routing.

ip policy {**load-balance|redundance**}

no ip policy

Parameter description

Parameter	Description
load-balance | redundance	Specify the policy: load balancing or redundant backup.

Default Redundant backup is adopted by default.

Command mode	Global configuration mode.
Usage guidelines	When you configure the **set ip next-hop** command in the sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first hop of the policy-based routing can be parsed. When the load balancing is set, multiple hops of the policy-based routing can be parsed. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops. The parsed next hop refers to the learned next hop of ARP message. Caution NPE80 do not support this command.

Examples

In the example below, there are multiple next hops configured in the route map. After the redundant backup is set in the global configuration mode, only the first next hop among the sub-route map of the policy-based routing applied on the interface FastEthernet 0/0 takes effect and performs forwarding.

Example1: set the ACL matched the IP packet

```
DES-7200(config)#access-list 1 permit 10.0.0.1
DES-7200(config)#access-list 2 permit 20.0.0.1
```

Example2: define the route map

```
DES-7200(config)#route-map lab1 permit 10
DES-7200(config-route-map)#match ip address 1
DES-7200(config-route-map)#set ip next-hop 196.168.4.6
DES-7200(config-route-map)#set ip next-hop 196.168.4.7
DES-7200(config-route-map)#set ip next-hop 196.168.4.8
DES-7200(config-route-map)#exit
DES-7200(config)#route-map lab1 permit 20
DES-7200(config-route-map)#match ip address 2
DES-7200(config-route-map)#set ip next-hop 196.168.5.6
DES-7200(config-route-map)#set ip next-hop 196.168.5.7
DES-7200(config-route-map)#set ip next-hop 196.168.5.8
DES-7200(config-route-map)#exit
```

Example3: apply the policy-based routing on the interface

```
DES-7200(config)#interface FastEthernet 0/0
DES-7200(config-if)#ip policy route-map lab1
DES-7200(config-if)#exit
DES-7200(config)#ip policy redundance
```

7.1.3 ip policy route-map

Use this command to enable the policy-based routing on an interface in the interface configuration mode. The **no** format of this command disables the function.

ip policy route-map *route-map*

no ip policy route-map

Parameter description

Parameter	Description
route-map	Name of the route map

Default Disabled.

Command mode Interface configuration mode.

Usage guidelines

The policy-based routing must be applied on the specified interface. That interface performs only the policy-based routing for the received packets, while the packets sent by the interface will be forwarded normally according to the routing table.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

Caution

Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Examples

In the example below, when the interface FastEthernet0/0 receives datagram, if the source address of the datagram is 10.0.0.1, it sets the next-hop as 196.168.4.6; if the source address is 20.0.0.1, it sets the next-hop as 196.168.5.6; otherwise, otherwise, the general forwarding will be performed.

Example1: set the ACL matched with the IP packets

```
DES-7200(config)#access-list 1 permit 10.0.0.1
DES-7200(config)#access-list 2 permit 20.0.0.1
```

Example2: define the route map

```
DES-7200(config)#route-map lab1 permit 10
DES-7200 (config-route-map)#match ip address 1
DES-7200(config-route-map)#set ip next-hop 196.168.4.6
```

```
DES-7200(config-route-map)#exit
DES-7200(config)#route-map lab1 permit 20
DES-7200(config-route-map)#match ip address 2
DES-7200(config-route-map)#set ip next-hop 196.168.5.6
DES-7200(config-route-map)#exit
```

Example3: apply the route map on the interface

```
DES-7200(config)#interface FastEthernet 0/0
DES-7200(config-if)#ip policy route-map lab1
DES-7200(config-if)#exit
```

Related commands

Command	Description
access-list	Define the access list rule.
route-map	Define the route map.
set vrf	Define the VRF instance of the policy-based IP packet.
set ip next-hop	Define the next hop of the policy-based routing.
set ip default next-hop	Define the default next hop of the policy-based routing.
set ip tos	Set the TOS in the head of the IP packet.
set ip dscp	Set the DSCP of the IP packet.
set ip precedence	Set the priority level in the head of the IP packet.
match ip address	Set the IP address.

7.2 Showing Related Commands

7.2.1 show ip policy

Use this command to view the interface configured the policy-based routing and the name of route map applied on the interface.

show ip policy

Parameter description

Parameter	Description
-	-

Default Settings	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples

```
DES-7200#show ip policy
Banlance Mode: redundance
Interface           Route map
local               test
FastEthernet 0/0    test
```

Related commands

Command	Description
ip policy route-map	Apply the policy-based routing on the interface.
ip local policy route-map	Apply the policy-based routing on the local interface.

8 VRF Commands

8.1 Configuration Related Commands

8.1.1 ip vrf

To create a VRF ,execute this command.The **no** form of this command deletes a VRF.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Parameter description

Parameter	Description
vrf-name	VRF name

Command mode

Global configuration mode

Usage Guideline

This command creates a VRF.

Examples

```
DES-7200# ip vrf redvrf
```

8.1.2 ip vrf forwarding

To add an interface or sub-interface to a VRF, execute this command. The **no** form of this command allows the interface or sub-interface quit the VRF.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Parameter description

Parameter	Description
vrf-name	Name of the VRF that the interface or sub-interface joins

Default configuration

By default, the interface does not belong to any VRF.

Command mode

Interface configuration mode

Usage Guideline

You can bind the interface to the uni-protocol IPv4 VRF without the IPv6 enabled on the interface.

On the device supporting the VRF, if the interface is bound to the uni-protocol IPv4 VRF with the IPv6 protocol enabled, the device cannot forward the IPv6 packets received on this interface.

Examples

```
DES-7200(config-if)# ip vrf forwarding redvrf
```

8.2 Show Related Command

8.2.1 show ip vrf

This command shows the VRF information.

show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]

Parameter description

Parameter	Description
brief	(Optional) Show the VRF information in brief.
detail	(Optional) Show the VRF information in detail.
interfaces	(Optional) Show the VRF's interface information in detail.

vrf-name	(Optional) Name of the VRF

Default configuration

All VRF information are displayed without parameter specified.

Command mode

Privileged EXEC mode

Usage Guideline

Use this command to show the VRF information, which can be divided into two levels：

- Use the keyword **brief** to show the information in brief.
- Use the keyword **detail** to show the information in detail.
- Use the keyword **interfaces** to show the VRF's interface information.

Examples

```
DES-7200# show ip vrf redvrf
```

DES-7200

Multicast Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 IPv4 Multicast Routing Commands

1.1 Configuration Related Commands:

1.1.1 clear ip mroute

Use this command to remove the forwarding information of the IP multicast routes.

clear ip mroute [**vrf** *vrf-name*] {***** | *group-address* [*source -address*]}

Parameter description

Parameter	Description
*	Remove all the forwarding information in the IP multicast route table.
vrf vrf-name	Specify the VRF instance
group-address	Group IP address of IP multicast routes.
source-address	Source IP address of multicast routess.

Command mode

Privileged mode.

Examples

Following example shows how to remove the entry whose group IP address is 230.0.0.1 from the multicast routing table:

```
DES-7200# clear ip mroute 230.0.0.1
```

Related commands

Command	Description
show ip mroute	Show the forwarding information of multicast routes.

1.1.2 clear ip mroute statistics

Use this command to remove the statistics of IP multicast routes.

clear ip mroute [**vrf** *vrf-name*] **statistics** {***** | *group-address* [*source-address*]}

Parameter description

Parameter	Description
*	Remove all the forwarding entries in the multicast route table.
group-address	Group IP address of IP multicast routes
vrf vrf-name	Specify the VRF instance
source-address	Source IP address of multicast route.

Command mode

Privileged mode.

Usage guideline

This command allows you to clear the statistics information of IP multicast routes.

Examples

Following example shows how to clear the statistics of entry with the group IP address 230.0.0.1 from the multicast routing table.

```
DES-7200# clear ip mroute statistics 230.0.0.1
```

Related commands

Command	Description
show ip mroute	Show the multicast route forwarding information.
clear ip mroute	Clear the multicast route forwarding information.

1.1.3 ip mroute

Use this command to configure static multicast routes. Use the **no** form of this command to delete the configured routes.

ip mroute [**vrf** *vrf-name*] *source-address mask* [*protocol as-number*] {*rpf-addrress* | *interface-type interface-number*} [*distance*]

no ip mroute [**vrf** *vrf-name*] *source-address mask* [*protocol as-number*] {*rpf-addrress* | *interface-type interface-number*} [*distance*]

Parameter description

Parameter	Description
source-address	Source IP address of the multicast route
vrf vrf-name	Specify the VRF instance
mask	Mask of the source IP address
protocol	(Optional) The unicast routing protocol being used.
rpf-address	Incoming interface of the multicast route
interface-type interface-number	Interface type and interface ID.
distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Default

distance: 0.

Command mode

Global configuration mode.

Usage guideline

This command is used to configure the route for the purpose of RFF check. Note that the configured route is prior to the route learned in the unicast form.

Examples

The following example allows the multicast routes of all the sources in a network to pass 172.30.10.13:

```
DES-7200(config)# ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
```

1.1.4 ip multicast boundary

Use this command to configure the boundary of an IP multicast group. The **no** form of this command removes the configured boundary.

ip multicast boundary *access-list*

no ip multicast boundary *access-list*

Parameter description

Parameter	Description
access-list	Access list associated with the multicast boundary.

Default

The boundary of a specified IP multicast group is defined by default.

Command mode

Interface configuration mode

Usage guideline

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IP address.

Note:

This command filters IGMP and PIMSM packets of the specified IP address range. Multicast packets will not be received and sent through the interface of the boundary.

Examples

The following example configures svi1 as the boundary of all IP multicast groups.

```
DES-7200(config)# ip access-list mul-boun
DES-7200(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255
DES-7200(config-std-nacl)#exit
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ip multicast boundary mul-boun
```

1.1.5 ip multicast route-limit

Use this command to limit the number of the entries that can be added to the multicast routing table.

ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

no ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

Parameter

Parameter	Description

description	*limit*	The number of the entries that can be added to the multicast routing table is 1 to 2147483647. The default value is 1024.
	vrf vrf-name	Specify the VRF instance
	threshold	(Optional) Number of multicast routes at which alarms will be triggered. The default value is 2147483647.

Default

The default value of *limit* is 1024.

The default value of *threshold* is 2147483647.

Command mode

Global configuration mode.

Usage guideline

This command is used to restrict the number of route adding to the IPv6 multicast table.

Note that the hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.

Examples

The following example sets the route limit to 500.

```
DES-7200(config)# ip multicast route-limit 500
```

1.1.6 ip multicast-routing

Use this command to enable multicast routing forwarding. The **no** form of this command disables multicast routing forwarding.

ip multicast-routing [**vrf** *vrf-name*]

no ip multicast-routing [**vrf** *vrf-name*]

Parameter description

Parameter	Description
vrf vrf-name	Specify the VRF instance

Default

Disabled.

Command mode	Global configuration mode.
Usage guideline	This command allows you to enable IPv4 multicast routing forwarding. The multicast protocol will not be enabled with IPv4 multicast routing forwarding disabled. It is not recommended to configure different v4 multicast routing protocols on different interfaces of a device.
Examples	This command enables multicast routing forwarding. `DES-7200(config)# ip multicast-routing`

1.1.7 ip multicast rpf longest-match

Select the multicast static routing, MBGP routing and unicast routing that could be used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules.

Use this command to select the one with the mask longest-matched from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.

The no form of this command restores it to the default setting. By default, select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.

ip multicast [**vrf** *vrf-name*] **rpf longest-match**

no ip multicast [**vrf** *vrf-name*] **rpf longest-match**

Parameter description

Parameter	Description
vrf vrf-name	Specify the VRF instance

Default	Select the multicast static routing, MBGP routing and unicast routing that are used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules. Then select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.
Command mode	Global configuration mode.
Examples	The following example configures to select the routing with the longest-match. `DES-7200(config)# ip multicast rpf longest-match`

1.1.8 ip multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. The **no** form of this command removes the setting.

ip multicast static *source-address group-address interface-type interface-number*

no ip multicast static *source-address group-address interface-type interface-number*

Parameter description

Parameter	Description
source-address	Source IP address
group-address	IP address of the multicast group
interface-type interface number	Layer 2 interface on which multicast packets are allowed to forward

Default	Disabled
Command mode	Global configuration mode

Usage guideline	You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces. This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-DM or PIM-SM) may be affected because some features of the multicast protocol are driven by multicast flows.

Examples	The following example configures forwarding multicast flows (192.168.43.4 and 255.1.1.5) through GigabitEthernet 2/6 and FastEthernet 3/2.
	`DES-7200(config)# ip multicast static 192.168.43.4 225.1.1.5 G2/6`
	`DES-7200(config)# ip multicast static 192.168.43.4 225.1.1.5 F3/2`

1.1.9 ip multicast ttl-threshold

Use this command to configure TTL (time-to-live) threshold on the interface. Use the **no** form of the command to restore it to the default value.

ip multicast ttl-threshold *ttl-value*

ip multicast ttl-threshold

Parameter description

Parameter	Description
ttl-value	TTL threshold on the interface, within the range of 0 to 255.

Default	The default *ttl-value* is 0.
Command mode	Interface configuration mode.

Usage guideline	Use **show running-config** to display configuration. A device with multicast enabled can maintain one TTL threshold for every interface. If the TTL of the multicast packet received is greater than the threshold of the interface, the packets will be forwarded. Otherwise, the packet is discarded. Note that the TTL threshold is effective only to the multicast frames. In addition, you must configure it on the L3 interface.
Examples	The following example sets the TTL threshold on the interface to 5. `DES-7200(config-if)# ip multicast ttl-threshold 5`

1.1.10 msf nsf

Use this command to configure the parameter for the continous multicast forwarding.

msf nsf {{convergence-time ***time***} | {leak ***interval***} }

no msf nsf {**convergence-time** | **leak**}

Parameter description

Parameter	Description
convergence-time *ttl-value*	Maximum time for the multicast protocol convergence, in the valid range of the 0-3600s.
leak *interval*	Packet multicast leak time, in the valid range of 0-3600s

Default	convergence-time : 20s; leak interval: 30s
Command mode	Global configuration mode.
Usage guideline	N/A

Examples	The following example shows how to set the maximum time for the protocol convergence.
	`DES-7200 (config)# msf nsf convergence-time 300`
	`DES-7200 (config)#`
	The following example shows how to set the packets leak time:
	`DES-7200(config)# msf nsf leak 200`
	`DES-7200(config)#`

1.1.11 msf ipmc-overflow override

Use this command to enable the overflow overriding mechanism.

msf ipmc-overflow override

no msf ipmc-overflow override

Parameter description

Parameter	Description
-	-

Default	Disabled.
Command mode	Global configuration mode.
Usage guideline	N/A

Examples	The following example shows how to enable the overflow overriding mechanism.
	`DES-7200 (config)# msf ipmc-overflow override`
	`DES-7200 (config)#`

1.2 Show Related Commands

1.2.1 show ip mroute

Use this command to show the multicast forwarding table.

show ip mroute [**vrf** *vrf-name*] [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]

Parameter description

Parameter	Description
group-address	Multicat group IP address
vrf vrf-name	Specify the VRF instance
group-or-source-address	Multicast or source IP address
group-or-source-address	Multicast or source IP address. The two addresses must not be the multicast addresses or source addresses at the samet time.
dense	Show PIM-DM multicast routing table.
sparse	Show PIM-SM multicast routing table.
summary	Show the summary of the multicast routing table.
count	Show the count of the multicast routing table.

Command mode

Privileged mode.

Examples

The following example shows the information of the multicast routing table:

```
DES-7200# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
```

```
FastEthernet 1/3
```

The following example shows the information of a specific entry:

```
DES-7200# show ip mroute 10.10.1.52 224.0.1.3
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires
00:01:28
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example shows the count of the routing table:

```
DES-7200# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10
Forwarding Counts: Pkt count/Byte count, Other Counts:
Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat
sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example shows the summary of the routing table:

```
DES-7200# show ip mroute summary
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM,
Flags: T
```

Field	Description

Flags	I-Immediate statistic T-Timed statistic F-Already set to the forwarding table
Timers:Uptime/Stat Expiry	Time when the entry is created. Time when it is aged.
Interface State	Interface state.
Owner	Owner of the entry, which may be a multicast routing protocol
Incoming interface	Expected packet incoming interface. If the actual incoming interface does not match it, the packets will be discarded.
Outgoing interface list	Outgoing interface list; the packets will be forwarded on the interfaces in the list.
Forwarding Counts: Pkt count/Byte count,	Forwarding count: packet count/byte count forwarded by the entry
Other Counts: Wrong If pkts	Count of the packets received from the wrong incoming interface.

Related commands

Command	Description
ip multicast-routing	Enabling the multicast routing forwarding.
ip pim dense-mode	Enable the PIM-DM on the interface.
ip pim sparse-mode	Enable the PIM-SM on the interface.

1.2.2 show ip mroute static

Use this command to show the v4 static multicast routing information.

show ip mroute [**vrf** *vrf-name*] **static**

Parameter description

Parameter	Description
vrf vrf-name	Specify the VRF instance

Command mode

Privileged mode.

Usage guideline

Use this command to show the user-configured static multicast routing. In the same conditions, the priority of the static multicast routing is higher than the dynamically learned.

Examples

The following example shows the information of the user-configured static multicast routing:

```
DES-7200#show ip mroute static
Mroute: 172.16.0.0, RPF neighbor: 172.30.10.13
Protocol: , distance: 0
```

1.2.3 show ip mvif

Use this command to show the basic information of the multicast interface.

show ip mvif [**vrf** *vrf-name*] { *interface-type interface-number* }

Parameter description

Parameter	Description
interface-type interface-number	Interface Type and number
vrf vrf-name	Specify the VRF instance

Command mode

Privileged mode.

Examples

The following example shows the basic information of the multicast interface of **svil**.

```
DES-7200#show ip mvif vlan 1
Interface      Vif   Owner      TTL  Local       Remote
Uptime
             Idx   Module     Address        Address
VLAN 1        1     PIM-DM      2   192.168.1.1   0.0.0.0
00:13:16
```

1.2.4 show ip rpf

Use this command to show the RPF information of the specified source IP address.

show ip rpf [**vrf** *vrf-name*] {*source-address* [*group-address*] [**rd** *route-distinguisher*]} [**metric**]

Parameter description

Parameter	Description
source-address	Specified source IP address
group-address	Specified source IP address
rd *route-disting unisher*	Use the RD provy for the serching.
metric	Show the metric of the MDT-SAFI route.
vrf vrf-name	Specify the VRF instance

Command mode

Privileged mode.

Examples

The following example shows the information of the RPF to 192.168.1.54:

```
DES-7200# show ip rpf 192.168.1.54
RPF information for 192.168.1.54
RPF interface: VLAN 1
RPF neighbor: 0.0.0.0
RPF route: 192.168.1.0/24
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0 RPF information for 192.168.1.54
RPF interface: VLAN 1
RPF neighbor: 0.0.0.0
RPF route: 192.168.1.0/24
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0
```

1.2.5 show ip mrf mfc

Use this command to show the IPv4 multicast routing forwarding table.

show ip mrf [**vrf** *vrf-name*] **mfc** [*soure-address group-address*]

Parameter description

Parameter	Description
vrf *vrf-name*	Private nework's VRF name, if no vrf name is specified, the public network's multicast routing forwarding entries are displayed by default.
source-address	Source address of the multicast routing forwarding entries.
group-address	Group address of the multicast routing forwarding entries.

Default

All IPv4 multicast routing forwarding entries are displayed by default.

Command mode

Privileged mode.

Usage guideline

The three parameters in this command are optional, wherein the source address and group address must be specified at the same time.

- If no source address and group address are specified, all mfc entries are displayed.
- When the source address and group address are specified only, the entries corresponding to the source and group addresses are displayed.

Examples

The following example shows all IPv4 layer-3 multicast routing forwarding entries with source address 20.0.1.30.

```
DES-7200#show ip mrf mfc 20.0.1.30 233.3.3.3

Multicast Routing and Forwarding Cache Table

(20.0.1.30, 233.3.3.3)

  FAST_SW, SWTCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099,
WRONG IF: 0
```

```
 Incoming interface: VLAN 1[4097]

Outgoing interface list:

   VLAN 3 (1)
```

The fields in the execution of the **show ip mrf mfc** command are described in the following table.

Field	Description
20.0.1.30	Source address of the entry.
233.3.3.3	Group address of the entry.
FAST_SW	The Flag shows whether to allow the fast forwarding or not. If the non-Ethernet interface, ppp, hdlc and frame relay exist, no fast forwarding entry generates.
SWTCHED	Indicate whether the entry configuration on the next layer forwarding table has done not not.
MIN_MTU MTU	The minimum MTU of the entry.
MIN_MTU_IFINDEX	The interface index with the minimum MTU value.
WRONG IF	The statistics number of the multicast data packets received on the wrong incoming interface.
Incoming interface	Incoming interface of the entry.
VLAN 3 (1)	The layer-3 outgoing interface of the entry is VLAN3. 1 for the ttl threshold of this layer-3 interface.

1.2.6 show msf msc

Use this command to show IPv4 multi-layer multicast forwarding table.

show msf msc [*soure-address*] [*group-address*] [*vlan-id*]

Parameter	Parameter	Description

description	*source-address*	Specified source IP address of the multi-layer multicast forwarding table.
	group-address	Specified group address of the multi-layer multicast forwarding table.
	vlan-id	The Vlan id where the incoming interface of the multi-layer multicast forwarding table is. 4096 indicates a routed port.

Default

All IPv4 multi-layer multicast forwarding entries are displayed by default.

Command mode

Privileged mode.

Usage guideline

The three parameters in this command are optional.

If no source address and group address are specified, all mfc entries are displayed.

- If only the source address is specified as s1, all msc entries with source address 1 are displayed.
- If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed.
- If the source address is specified as s1, the group address as g1 and the vlan id as v1, all corresponding msc entries are displayed.
- Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.

Examples

The following example shows the IPv4 layer-3 multicast forwarding entries with source IP address 192.168.195.25:

```
DES-7200# show msf msc 192.168.195.25

Multicast Switching Cache Table

(192.168.195.23, 233.3.3.3, 1), SYNC, MTU:0, 1 OIFs
```

```
VLAN 1(0): 1 OPORTs, REQ: DONE

OPORT 6, IGMP-SNP, REQ: DONE
```

The fields in the execution of the **show mrf mfc** command are described in the following table.

Field	Description
192.168.195.23	Source address of the entry.
233.3.3.3	Group address of the entry.
1	Vlan id where the incoming interface of the entry is.
SYNC	The entry has been synchronized to the hardware.
MTU	MTU value
OIFs	Layer-3 outgoing interface number.
VLAN1(0)	The vlan where the layer-3 outgoing interface oif is.
1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.
REQ: DONE	This oif configuration on the hardware has done.
OPORT 6	The layer-2 port in the oif with index 6.
IGMP-SNP	This port is created by the IGMP SNOOPING protocol. This value can also be the PIM-SNP, which means this port is created by the PIM SNOOPING protocol. And the ROUTER means this port is created by the layer-3 protocol.
REQ: DONE	The port configuration on the hardware has done.

1.2.7 show msf nsf

Use this command to show the configuration of continuous multicast forwarding.

show msf nsf

Parameter description

Parameter	Description
-	-

Command mode

Privileged mode.

Examples

The following example shows the configuration of continuous multicast forwarding.

```
DES-7200# show msf nsf

Multicast HA Parameters

-------------------------------------------------+-----
-+

protocol convergence timeout                    120 secs

flow leak interval                             20 secs

DES-7200#
```

Related commands

Command	Description
msf nsf	Configure the multicast NSF parameter.

1.3 Debugging Related Commands

1.3.1 debug nsm mcast all

Use this command to turn on all multicast debugging switches. The **no** form of this command turns off all the debugging switches.

debug nsm mcast [**vrf** *vrf-name*] **all**

Parameter description

Parameter	Description
vrf vrf-name	Specify the VRF instance

Default

Disabled

Command mode	Privileged EXEC configuration mode
Usage guideline	Turning on all multicast debugging switches to check related running process.
Examples	The following example turns on all the multicast debugging switches. `DES-7200# debug nsm mcast all`

1.3.2 debug nsm mcast fib-msg

Use this command to turn on the fib-msg debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast [**vrf** *vrf-name*] **fib-ms**

Parameter description

Parameter	Description
vrf vrf-name	Specify the VRF instance

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the fib-msg debugging switch. `DES-7200# debug nsm mcast fib-msg`

1.3.3 debug nsm mcast register

Use this command to turn on the register debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast [**vrf** *vrf-name*] **register**

Parameter

Parameter	Description

description	**vrf** vrf-name	Specify the VRF instance

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the register debugging switches. `DES-7200# debug nsm mcast register`

1.3.4 debug nsm mcast stats

Use this command to turn on the interface statistics debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast [**vrf** *vrf-name*] **stats**

Parameter description	**Parameter**	**Description**
	vrf vrf-name	Specify the VRF instance

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the interface statistics debugging switches. `DES-7200# debug nsm mcast stats`

1.3.5 debug nsm mcast vif

Use this command to turn on the VIF debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast [**vrf** *vrf-name*] **vif**

Parameter description

Parameter	Description
vrf vrf-name	Specify the VRF instance

Default Disabled

Command mode Privileged EXEC configuration mode

Usage guideline N/A

Examples The following example turns on the VIF debugging switches.

```
DES-7200# debug nsm mcast vif
```

1.3.6 debug nsm mcast mrt

Use this command to turn on the MRT debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast [**vrf** *vrf-name*] **mrt**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF instance.

Default Disabled

Command mode Privileged EXEC configuration mode

Usage guideline N/A

Examples	The following example turns on the MRT debugging switches. `DES-7200# debug nsm mcast mrt`

1.3.7 debug ip mrf forwarding

Use this command to turn on the debugging switch to show the operation of the IPv4 multicast forwarding. The **no** form of this command turns off the debugging switch.

debug ip mrf [vrf *vrf-name*] forwarding

no debug ip mrf [**vrf** *vrf-name*] **forwarding**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF instance.

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the debugging switches to show the operation of forwarding the IPv4 multicast message. `DES-7200# debug ip mrf forwarding`

1.3.8 debug ip mrf mfc

Use this command to turn on the debugging switch to show the operation of IPv4 multicast routing forwarding entries. The **no** form of this command turns off the debugging switch.

debug ip mrf [vrf ***vrf-name***] mfc

no debug ip mrf [**vrf** *vrf-name*] **mfc**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF instance.

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the debugging switches to show the operation of IPv4 multicast routing forwarding entries. `DES-7200# debug ip mrf mfc`

1.3.9 debug ip mrf event

Use this command to turn on the debugging switch to show the operateion of IPv4 multicast routing forwarding event. The **no** form of this command turns off the debugging switch.

debug ip mrf [vrf ***vrf-name***] event

no debug ip mrf [**vrf** *vrf-name*] **event**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF instance.

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the debugging switches to show the IPv4 multicast routing forwarding event. `DES-7200# debug ip mrf event`

1.3.10 debug msf forwarding

Use this command to turn on the debugging switch to show the operation of IPv4 multi-layer multicast forwarding. The **no** form of this command turns off the debugging switch.

debug msf forwarding

no debug msf forwarding

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the debugging switches to show the operation of IPv4 multi-layer multicast forwarding. `DES-7200# debug msf forwarding`

1.3.11 debug msf mfc

Use this command to turn on the debugging switch to show the operation of IPv4 multi-layer multicast forwarding entries. The **no** form of this command turns off the debugging switch.

debug msf mfc

no debug msf mfc

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the debugging switches to show the operation of IPv4 multi-layer multicast forwarding. `DES-7200# debug msf mfc`

1.3.12 debug msf ssp

Use this command to turn on the debugging switch to show the operation of IPv4 multi-layer multicast forwarding hardware. The **no** form of this command turns off the debugging switch.

debug msf ssp

no debug msf ssp

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the debugging switches to show the IPv4 multi-layer multicast forwarding. `DES-7200# debug msf ssp`

1.3.13 debug msf api

Use this command to turn on the debugging switch to show the calling operation of the api interface provided by the IPv4 multi-layer multicast forwarding. The **no** form of this command turns off the debugging switch.

debug msf forwarding

no debug msf forwarding

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	`DES-7200# debug msf api`

1.3.14 debug msf event

Use this command to turn on the debugging switch to show the operation of the IPv4 multi-layer multicast forwarding event. The **no** form of this command turns off the debugging switch.

debug msf event

no debug msf event

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	`DES-7200# debug msf event`

2 IPv6 Multicast Routing Commands

2.1 Configuration Related Commands

2.1.1 clear ipv6 mroute

Use this command to remove the specific or all IPv6 multicast forwarding entries.

clear ipv6 mroute { ***** | *v6group-address* [*v6source -address*]}

Parameter description

Parameter	Description
*	Remove all the forwarding information in the IPv6 multicast route table.
v6group-address	Group IPv6 address of IPv6 multicast routes.
v6source-address	Source IPv6 address of multicast routess.

Command mode

Privileged mode.

Examples

Following example shows how to remove all the multicast routing entries:

```
DES-7200# clear ip mroute *
```

Related commands

Command	Description
show ipv6 mroute	
clear ipv6 mroute statistics	

2.1.2 clear ipv6 mroute statistics

Use this command to remove the statistics of IPv6 multicast routes.

clear ipv6 mroute statistics {***** | *v6group-address* [*v6source -address*]}

Parameter description

Parameter	Description
*	Remove all the forwarding entries in the multicast route table.
v6group-address	Group IPv6 address of IPv6 multicast routes
v6source-address	Source IPv6 address of multicast route.

Command mode

Privileged mode.

Usage guideline

This command allows you to clear the statistics information of IPv6 multicast routes.

Examples

Following example shows how to clear all the statistical information of the multicast routing entries.

```
DES-7200# clear ip mroute statistics *
```

Related commands

Command	Description
show ipv6 mroute	Show the multicast route forwarding information.
clear ipv6 mroute	Clear the multicast route forwarding information.

2.1.3 ipv6 mroute

Use this command to configure static IPv6 multicast routes. Use the **no** form of this command to delete the configured routes.

ipv6 mroute ipv6-prefix/prefix-length [protocol as-number] {v6rpf-addrress | interface-type interface-number} [distance]

no ipv6 mroute ipv6-prefix/prefix-length [protocol as-number] { v6rpf-addrress | interface-type interface-number} [distance]

Parameter

Parameter	Description

description

ipv6-prefix/prefix-length	Source IPv6 address of the multicast route.
mask	Mask of the source IPv6 address.
protocol	(Optional) The unicast routing protocol being used.
v6rpf-address	Incoming interface of the multicast route
interface-type *interface-number*	Interface type and interface ID.
distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Default

The static IPv6 multicast routing is not configured.

Command mode

Global configuration mode.

Usage guideline

This command is used to configure the route for the purpose of RFF check. Note that the configured route is prior to the route learned in the unicast form.

If the outgoing direction of static multicast route but not the next-hop IP shall be specified, the outgoing direction must be of the point-to-point type.

The RPF rule is that when a best multicast route from the multicast list is selected, if the BGP multicast route and the static multicast route coexist, the latter one takes the precedence; select a best unicast route from the unicast list and compare the mask length of the best multicast and unicast routes, the one with greater mask length becomes the RPF route; if both mask length are the same, you shall compare the distance, and the one with smaller distance becomes the RPF route; if both distance values are the same, the multicast route becomes the RPF route.

Examples

The following example allows the static multicast route 2233::/64 to pass 3333::3333:

```
DES-7200(config)# ipv6 mroute 2233:: /64 3333::3333
```

2.1.4 ipv6 multicast boundary

Use this command to configure the boundary of an IPv6 multicast group. The **no** form of this command removes the configured boundary.

ipv6 multicast boundary *access-list-name*

no ipv6 multicast boundary *access-list-name*

Parameter description

Parameter	Description
access-list-name	Access list associated with the multicast boundary.

Default

The boundary of a specified IPv6 multicast group is defined by default.

Command mode

Interface configuration mode.

Usage guideline

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IPv6 address.

Caution

This command filters MLD、PIM-SMv6 packets of the specified IPv6 address range. Multicast packets will not be received and sent through the interface of the boundary.

Examples

The following example configures svi1 as the boundary of all IPv6 multicast groups.

```
DES-7200(config)# ip access-list mul-boun
DES-7200(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255
DES-7200(config-std-nacl)#exit
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ip multicast boundary mul-boun
```

2.1.5 ipv6 multicast route-limit

Use this command to limit the number of the entries that can be added to the IPv6 multicast routing table.

ipv6 multicast route-limit *limit* [*threshold*]

no ipv6 multicast route-limit *limit* [*threshold*]

Parameter description

Parameter	Description
limit	The number of the entries that can be added to the IPv6 multicast routing table is 1 to 2147483647. The default value is 1024.
threshold	(Optional) Number of IPv6 multicast routes at which alarms will be triggered. The default value is 2147483647.

Default

The default value of *limit* is 1024.

The default value of *threshold* is 2147483647.

Command mode

Global configuration mode.

Usage guideline

This command is used to restrict the number of route adding to the IPv6 multicast table.

Caution

The hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.

Examples

The following example sets the route limit to 500 and the warning value 90.

```
DES-7200(config)# ipv6 multicast route-limit 500 90
```

2.1.6 ipv6 multicast-routing

Use this command to enable the IPv6 multicast routing forwarding. Use the **no** form of the command to disable this function.

ipv6 multicast-routing

no ipv6 multicast-routing

Parameter description

Parameter	Description
-	-

Default

Disabled

Command mode

Global configuration mode.

Usage guideline

Use this command to enable the IPv6 multicast routing forwarding. With this function disabled, the multicast protocol cannot be enabled.

Caution

This command must be configured to enable the IPv6 multicast routing forwarding. This function conflicts with IGMP Snooping.

Examples

The following example enables the IPv6 multicast routing forwarding.

```
DES-7200(config)# ipv6 multicast-routing
```

2.1.7 ipv6 multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. The **no** form of this command removes the setting.

ipv6 multicast static *source-address group-address interface-type interface-number*

no ipv6 multicast static *source-address group-address interface-type interface-number*

Parameter description

Parameter	Description
source-address	Source IPv6 address

	group-address	IPv6 address of the multicast group
	interface-type interface number	Layer 2 interface on which multicast packets are allowed to forward

Default	Disabled
Command mode	Global configuration mode
Usage guideline	You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces. This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-SMv6) may be affected because some features of the multicast protocol are driven by multicast flows.

Examples	The following example configures forwarding multicast flows (2222::3333，ff66::100) through GigabitEthernet 2/6 and FastEthernet 3/2.
	`DES-7200(config)# ipv6 multicast static 2222::3333 ff66::100 G2/6`
	`DES-7200(config)# ipv6 multicast static 2222::3333 ff66::100 F3/2`

2.1.8 ipv6 multicast rpf longest-match

Use the RPF rule to select the static multicast route, MBGP route and the unicast route for the purpose of RPF check from the static multicast route list, the MBGP route list and the unicast route list.

Use this command to select one route with the longest-matched mask from the above-mentioned three routes. If the priority values of all three routes are the same, the routes will be selected in order of static multicast route, MBGP route and unicast route.

Use the **no** form of this command to restore it to the default value.

ipv6 multicast rpf longest-match

no ipv6 multicast rpf longest-match

Parameter description

Parameter	Description
-	-

Default

Use the RPF rule to select the static multicast route, MBGP route and the unicast route for the purpose of RPF check from the static multicast route list, the MBGP route list and the unicast route list.

Use this command to select one route, which is prior to the other two routes, with the longest-matched mask from the above-mentioned three routes. If the priority values of all three routes are the same, the routes will be selected in order of static multicast route, MBGP route and unicast route.

Command mode

Global configuration mode

Usage guideline

N/A.

Examples

```
DES-7200(config)# ipv6 multicast rpf longest-match
```

2.2 Show Related Commands

2.2.1 show ipv6 mroute

Use this command to show the IPv6 multicast forwarding table.

show ipv6 mroute [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]

Parameter description

Parameter	Description
v6group-address	Multicat group IPv6 address

v6source-address	Multicast source IPv6 address
summary	Show the summary of the multicast routing table.
count	Show the count of the multicast routing table.

Command mode

Privileged mode.

Examples

The following example shows all information of the IPv6 multicast routing table:

```
DES-7200# show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SMv6, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example shows the count of the routing table:

```
DES-7200# show ipv6 mroute count
IPv6 Multicast Statistics
Total 1 routes using 168 bytes memory
Route limit/Route threshold: 1024/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 77/147/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 77/147/0
Immediate/Timed stat updates sent to clients: 0/29
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:09
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
```

```
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(2222::1234, ff56::1234), Forwarding: 1/0, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following example shows the summary of the routing table:

```
DES-7200# show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), 00:00:28/00:03:25, PIM-SMv6, Flags: TF
```

Related commands

Command	Description
-	-

2.2.2 show ipv6 rpf

Use this command to show the RPF information of the specified source IPv6 address.

show ipv6 rpf {*v6source-address*}

Parameter description

Parameter	Description
V6source-address	Specified source IPv6 address

Command mode

Privileged mode.

Examples

The following example shows the information of the RPF to 2222::3333:

```
DES-7200# show ipv6 rpf 2222::3333
  RPF interface: GigabitEthernet 0/1
```

```
RPF neighbor: ::
RPF route: 2222::/64
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0
```

2.2.3 show ipv6 mroute static

Use this command to show the static IPv6 multicast routing information.

show ipv6 mroute static

Parameter description

Parameter	Description
-	-

Command mode

Privileged mode.

Usage guideline

This command is used to show the statically-configured multicast route. Under the same condition, the static multicast route is prior to the unicast route.

Examples

The following example shows the static IPv6 multicast routing information:

```
DES-7200#show ipv6 mroute static
Mroute: 2233::/64, RPF neighbor: 3333::3333
  Protocol: , distance: 0
```

2.2.4 show ipv6 mvif

Use this command to show the basic information of the multicast interface.

show ipv6 mvif { *interface-type interface-number* }

Parameter description

Parameter	Description
interface-type interface-number	Interface Type and number

Command mode	Privileged mode.

Examples

The following example shows the basic information of the multicast interface of **svil**.

```
DES-7200#show ipv6 mvif
Interface             Mif   Owner          Uptime
                      Idx   Module
Register              0                  03d03h09m
VLAN 1                 1    PIMSMV6         03d03h09m
```

2.3 Debugging Related Commands

2.3.1 debug nsm mcast6 all

Use this command to turn on all IPv6 multicast debugging switches. The **no** form of this command turns off all the debugging switches.

debug nsm mcast6 all

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	Turning on all IPv6 multicast debugging switches to check related running process.

Examples

The following example turns on all the multicast debugging switches.

```
DES-7200# debug nsm mcast6 all
```

2.3.2 debug nsm mcast6 fib-msg

Use this command to turn on the fib-msg debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast6 fib-msg

Default	Disabled

Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the fib-msg debugging switch. `DES-7200# debug nsm mcast6 fib-msg`

2.3.3 debug nsm mcast6 register

Use this command to turn on the register debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast6 register

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the register debugging switches. `DES-7200# debug nsm mcast6 register`

2.3.4 debug nsm mcast6 stats

Use this command to turn on the interface statistics debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast6 stats

Default	Disabled

Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the interface statistics debugging switches. `DES-7200# debug nsm mcast6 stats`

2.3.5 debug nsm mcast6 vif

Use this command to turn on the VRF debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast6 vif

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the VRF debugging switches. `DES-7200# debug nsm mcast6 vrf`

3 IGMP Commands

3.1 Configuration Related Commands

3.1.1 ip igmp access-group

Use this command to control a multicast group on the interface. The **no** form of this command disables this function.

Command syntax

ip igmp access-group *access-list*

no ip igmp access-group

Parameter description

Parameter	Description
access-list	Name of access control list within the range of 1 to 199, 1300 to 2699, or characters.

Default

Filtering conditions are not set.

Command mode

Interface configuration mode.

Usage guidelines

You can add several multicast groups into the specific interfaces of the host in a subnet. These multicast groups can be controlled using **ip igmp access-group**.

With the IGMPv3 enabled, when the multicast group accesses the control command, the extended ACL is associated. If the IGMP report information received is (S1,S2,S3…Sn,G), the corresponding ACL will be used by this command to the (0, G) for the matching chek. In order to use this command normally, the (0,G) must be configured explicitly for the extended ACL so as to implement the normal filtering of (S1, S2, S3…Sn,G).

In the following example, the host service can only add the interface Ethernet 0/1 to the group 225.2.2.2 .

```
DES-7200# configure terminal
DES-7200(config)# access-list 1 permit 225.2.2.2 0.0.0.0
DES-7200(config)# interface ethernet 0/1
DES-7200(config-if)# ip igmp access-group 1
```

Examples

In the following example, associate the group control list with the extended ACL on the interface Eth 0/1 which only processes the igmp protocol packets with source address 1.1.1.1 and group address 233.3.3.3.

```
DES-7200# configure terminal
DES-7200(config)# ip access-list extended ext_acl
DES-7200(config-ext-nacl)# permit ip host 1.1.1.1 host 233.3.3.3
DES-7200(config)# interface ethernet 0/1
DES-7200(config-if)# ip igmp access-group ext_acl
```

3.1.2 ip igmp immediate-leave group-list

In the IGMPversion2 and IGMPversion3 versions, use this command to shorten the delay of leaving a group. This command is used when a single receiving host is connected to a single interface. The **no** form of this command is used to disable this function.

Command syntax

ip igmp immediate-leave group-list *access-list*

no ip igmp immediate-leave group-list

Parameter description

Parameter	Description
access-list	Name of access control list.

Default

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

If this command is not configured, the device will send a particular group query message upon receiving the leaving message from the interface. When the host response is timeout, the device stops forwarding packets to this interface. The length of timeout depends on the query

	interval of the last member and IGMP robustness variable. The default value is 2s. If this command is configured, the device does not send a particular group query message upon receiving the leaving message from the interface. Instead, it directly removes this interface from the IGMP buffer and notifies the IGMP protocol. This will shorten the time significantly.

Examples	The following example demonstrates how to provide the immediate leaving function for some multicast groups. Certainly, you must make sure each interface of these multicast groups have one group member only.
	`DES-7200# configure terminal`
	`DES-7200(config)# access-list 1 permit 225.192.20.0 0.0.0.255`
	`DES-7200(config)# interface ethernet 0/1`
	`DES-7200(config-if)# ip igmp immediate-leave group-list 1`
	`DES-7200(config-if)# exit`

Related commands	**ip igmp last-member-query-interval.**

3.1.3 ip igmp join-group

Use this command to configure the interface of the switch with host activities and adds it to a multicast group, so that the sub-switch can learn the corresponding group information. You can use this command to add an interface to a group. The **no** form of this command removes the setting.

Command Syntax	**ip igmp join-group** *group-address* **no ip igmp join-group** *group-address*

Parameter description

Parameter	Description
group-address	Multicast group IP address

Default configuration	The interface is not manually added to the multicast group.
Command mode	Interface configuration mode.

Usage guidelines	This command enables the host activities for the IGMP interface. When the host function is enabled, the interface can initiate the report message and respond to the query message. If the IGMP function is enabled on the interface, the interface can initiate the report message, so that the interface can learn the configured group members. You can use this command to add an interface to a group.

Examples	Following example is to add a host group member manually:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface fast 0/1`
	`DES-7200(config-if)# ip igmp join-group 233.3.3.3`

3.1.4 ip igmp last-member-query-count

last-member-query-count means the number of query packets that the multicast device will send continuously upon receiving the leave message. Use this command to configure the value of **last-member-query-count**. Use the **no** command to restore it to the default value.

Command syntax

ip igmp last-member-query-count *number*

no ip igmp last-member-query-count

Parameter description

Parameter	Description
number	Value of the last member query count in the range 2 to 7.

Default

The default value of **last-member-query-count** is 2.

Command mode

Interface configuration mode.

Usage guidelines

When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **last-member-query-count** time. The device will delete information about this group member if no group member report is received within the waiting

	time.

Examples	Set the value of last member query count to 3.
	`DES-7200# configure terminal`
	`DES-7200(config)# interface ethernet 0`
	`DES-7200(config-if)# ip igmp last-member-query-count 3`

3.1.5 ip igmp last-member-query-interval

Use this command to set the time interval of sending the group query message. Use the **no** form of this command to restore it to the default.

Command syntax	**ip igmp last-member-query-interval** *interval* **no ip igmp last-member-query-interval**

Parameter description

Parameter	Description
Interval	The interval sending the group query message in the range1 to 255(in the unit of 0.1 second).

Default	1s.
Command mode	Interface configuration mode.
Usage guidelines	When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **last-member-query-count** time. The device will delete information about this group member if no group member report is received within the waiting time.

Examples	The following example sets the interval of sending the group query message to 20 seconds:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface eth 0`
	`DES-7200(config-if)# ip igmp last-member-query-interval 200`

Related commands	**ip igmp immediate-leave.**

3.1.6 ip igmp limit (global configuration)

Use this command to globally set the maximum number of IGMP group records. Use the **no** form of this command to remove the setting.

Command syntax

ip igmp [**vrf** *vrf-name*] **limit** *number* [**except** *access-list*]

no ip igmp limit

Parameter description

Parameter	Description
number	Maximum number of IGMP states, depending on devices
vrf *vrf-name*	Specify the VRF.
except	(Optional) Prevent the groups of the access list from taking part in calculation.
access-list	(Optional) Acdess list name

Default

65536, the default value depends on the specific device.

Command mode

Global configuration mode.

Usage guidelines

Use this command to globally configure the maximum number of IGMP group records. The messages of the members exceeding the threshold will not be saved in the IGMP buffer and will not be forwarded.

This command can be configured globally or on the interface The messages of the members will be ignored if they exceed the interface or global configuration.

Examples

The following example sets the maximum number to 300:

```
DES-7200(config) # ip igmp limit 300
```

3.1.7 ip igmp limit (interface configuration)

Use this command to set the maximum number of IGMP states on the interface. Use the **no** form of this command to remove the setting.

Command syntax

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit

Parameter description

Parameter	Description
number	Maximum number of IGMP states, depending on devices.
except	(Optional) Prevent the groups of the access list from taking part in calculation, which is not limited by maximum number.
access-list	(Optional) Access list

Default 1024

Command mode Interface configuration mode.

Usage guidelines

This command in global configuration mode limits the number of the IGMP group members. The messages of the members over the limit are not recorded and processed.

This command can be configured globally or on the interface The messages of the members will be ignored if they exceed the interface or global configuration.

Examples

The following example sets the limitation to 300:

```
DES-7200(config-if)# ip igmp limit 300
```

3.1.8 ip igmp mroute-proxy

Use this command to configure an interface as a mroute-proxy interface that can transmit messages to its uplink ports.

Command syntax

ip igmp mroute-proxy *interfname*

no ip igmp mroute-proxy

Parameter description

Parameter	Description
interfname	Name of the relevant uplink interface.

Default configuration N/A.

Command mode	Interface configuration mode.
Usage guidelines	After an uplink interface is configured as **proxy-service** interface, the interface can forward the IGMP messages sent by other members.
Examples	Configure an interface to **mroute-proxy** interface: `DES-7200(config-if)# ip igmp mroute-proxy fa 0/1`

3.1.9 ip igmp proxy-service

Use this command to enable the service function of all downlink **mroute-proxy** ports. If you run this command on an interface, the interface becomes the uplink port of the corresponding **mroute-proxy** that associates its downlink ports and maintains the group information reported by the downlink ports.

Command syntax	**ip igmp proxy-service** **no ip igmp proxy-service**
Default configuration	All interfaces are not in the **proxy-serice** status.
Command mode	Interface configuration mode.
Usage guidelines	The command can configure at most 32 proxy-service ports. The number of interface with IGMP Proxy enabled is limited by the supported multicast interface number. When receiving a query message, the **proxy-service** port responds according to the IGMP group member information maintained by the port itself. The member information maintained by the **proxy-service** port is collected from the interface configured with **mroute-proxy**. Therefore, if a port is configured with proxy-service, the port performs the host activities, but not the device activities. If **switchport** operation is performed on an interface with proxy-service command configured, the **ip igmp mroute-proxy interface** command configured on the associated downlink ports is automatically deleted.

Examples	Configure an interface to the **proxy-service** module: `DES-7200(config-if)# ip igmp proxy-service`

3.1.10 ip igmp query-interval

Use this command to configure the query interval of an ordinary member. Use the **no** form to set the query interval of ordinary member to the default value.

Command syntax	**ip igmp query-interval** *seconds* **no ip igmp query-interval**

Parameter description

Parameter	Description
seconds	Query interval of ordinary member, in second. The range is 1 to 18000s.

Default	125s.
Command mode	Interface configuration mode.
Usage guidelines	The time to query an ordinary member can be changed by configuring the query interval of the ordinary member.

Examples	Configure the query interval of ordinary member to 120s on the interface Ethernet 0.
	`DES-7200(config-if)# ip igmp query-interval 120`
	Configure the query interval of ordinary member to the default value on the interface Ethernet 0.
	`DES-7200(config-if)# no ip igmp query-interval`

3.1.11 ip igmp query-max-response-time

Use this command to configure the maximum response interval. The **no** form of this command to set the maximum response interval to the default value.

Command syntax	**ip igmp query-max-response-time** *seconds* **no ip igmp query-max-response-time**

Parameter description

Parameter	Description
seconds	The maximum response interval, in second. The range is 1 to 25s.

Default	10s.
Command mode	Interface configuration mode.
Usage guidelines	This command controls the interval for the respondent to respond the query message before the device deletes the group information.

Examples	Configure the maximum response interval to 20s on the interface Ethernet 0.
	`DES-7200(config-if)# ip igmp query-max-response-time 20`
	Configure the maximum response interval to the default value on the interface Ethernet 0.
	`DES-7200(config-if)# no ip igmp query-max-response-time`

3.1.12 ip igmp query-timeout

Use this command to configure the time the device waits before it takes over as the querier. Use the **no** form to restore it to the default.

Command syntax	**ip igmp query-timeout** *seconds* **no ip igmp query-timeout**

Parameter description

Parameter	Description
seconds	Time the device waits before it takes over as the querier, in second. The range is 60 to 300s.

Default	255s.
Command mode	Interface configuration mode.
Usage guidelines	IGMPv2 should be run for this command to work. By default, Cisco sets the waiting time of the device to two times of the query interval of **ip igmp query-interval**. In DES-7200, the default value is set to 255s. This device becomes the querier if no query packet is received in this

	duration.

Examples	Configure the time the device waits before it takes over as the querier to 200s on the interface Ethernet 0/1.
	`DES-7200(config-if)# ip igmp query-timeout 200`
	Configure the time the device waits before it takes over as the querier to the default value on the interface Ethernet 0/1.
	`DES-7200(config-if)# no ip igmp query-timeout`

3.1.13 ip igmp robustness-variable

Use this command to change the value of the robustness variable. Use the **no** form of this command to restore it to the default value.

Command syntax	**ip igmp robustness-variable** *number* **no ip igmp robustness-variable**

Parameter description

Parameter	Description
number	The value of robustness variable ranging 2 to 7.

Default	The default value is 2.
Command mode	Interface configuration mode.

Examples	The following example sets the value of robustness variable to 3:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface ethernet 0`
	`DES-7200(config-if)# ip igmp robustness-variable 3`

3.1.14 ip igmp ssm-map enable

Use this command to enable the **igmp ssm-map** function in the global configuration mode. Use the **no** form of this command to disable the function.

Command syntax	**ip igmp** [**vrf** *vrf-name*] **ssm-map enable** **no ip igmp** [**vrf** *vrf-name*] **ssm-map enable**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

If this command is configured, the dynamically learned group information is added forcibly to the associated source record. This command is usually used together with the **ip igmp ssm-map static** command.

Examples

Enable the **igmp ssm-map** function in the global configuration mode:

DES-7200(config)# **ip igmp ssm-map enable.**

3.1.15 ip igmp ssm-map static

Use this command to map the static **ssm-map** source IP address to the group records in the global mode. Use the **no** form of this command to disable the function.

Command syntax

ip igmp [**vrf** *vrf-name*] **ssm-map static** *access-list a.b.c.d*

no ip igmp [**vrf** *vrf-name*] **ssm-map static** *access-list a.b.c.d*

Parameter description

Parameter	Description
access-list	ACL name in the range 1 to 99, 1300 to 1999 or characters.
vrf *vrf-name*	Specify the VRF.
a.b.c.d	Unicast address mapped to the group record.

Default configuration

N/A.

Command mode	Global configuration mode.
Usage guidelines	This command is used together with the **ip igmp ssm-map enable** command. After configuration, the port maps the corresponding source IP address to all received messages below **v3**.
Examples	Map the source address 192.168.2.2to all group records permitted by ACL 11 : `DES-7200(config)# ip igmp ssm-map static 11 192.168.2.2.`

3.1.16 ip igmp static-group

Use this command to directly add an interface to a group. You can use this command to add an interface to a group. Use the **no** form of this command to remove the setting.

Command Syntax	**ip igmp static-group** *group-address* **no ip igmp static-group** *group-address*

Parameter description

Parameter	Description
group-address	Multicast group IP address.

Default configuration	The switch is not added to the multicast group manually.
Command mode	Interface configuration mode.
Usage guidelines	This command directly adds an interface to a multicast group. The difference from **join-group** is that it directly adds an interface to the group without interacting with a report message. You can use this command to add an interface to a group.

Examples

Following example is to add a host group member manually:

```
DES-7200# configure terminal
DES-7200(config)# interface fast 0/1
DES-7200(config-if)# ip igmp static-group 233.3.3.3
```

3.1.17 ip igmp version

Use this command to set the version number of IGMP to be used on the interface. Use the **no** form of this command to restore it to the default value.

Command syntax

ip igmp version {**1** | **2** | **3**}

no ip igmp version

Parameter description

Parameter	Description
{**1** | **2** | **3**}	Three version numbers, ranging 1 to 3.

Default

The version number is 2 by default.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to globally configure the IGMP version. It should be noted that IGMP will reset after configuration.

Examples

The following example sets the version number to 2:

```
DES-7200# configure terminal
DES-7200(config)# interface ethernet 0
DES-7200(config-if)# ip igmp version 2
```

3.2 Show Related Commands

3.2.1 clear ip igmp group

Use this command to clear dynamic group member information obtained from the response messages in the IGMP buffer.

Command Syntax

clear ip igmp [**vrf** *vrf-name*] **group** [*group-address* [*interface-type interface-number*]]

Parameter description

Parameter	Description
N/A	Delete all group information.
group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
vrf *vrf-name*	Specify the VRF.
interface-type	Interface type.
interface-number	Interface number.

Command mode

Privileged mode.

Usage guidelines

The IGMP buffer includes a list that contains the multicast groups that the hosts in the direct subnet join. If the device joins a group, this group will be included in this list. To delete all the entries from the IGMP buffer, use the **clear ip igmp group** command without parameters.

Examples

Delete all group entries:

```
DES-7200# clear ip igmp group
```

Related commands

show ip igmp groups
show ip igmp interface

3.2.2 clear ip igmp interface

Use this command to clear the IGMP entry for the interface.

Command syntax

clear ip igmp [**vrf** *vrf-name*] **interface** *ifname*

Parameter description

Parameter	Description
ifname	Name of the interface
vrf *vrf-name*	Specify the VRF.

Default

N/A.

Command mode	Privileged mode.
Usage guidelines	This command is used to clear the information on the interface that is generated when IGMP is configured.
Examples	`DES-7200# clear ip igmp interface gigabitEthernet 4/1`

3.2.3 show ip igmp groups

Use this command to show the groups directly connected to the device and the group information learnt from IGMP.

Command syntax

show ip igmp [**vrf** *vrf-name*] **groups** [*group-address* | *interface-type*
interface-number] [**detail**]

Parameter description

Parameter	Description
group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
vrf *vrf-name*	Specify the VRF.
interface-type	Interface type.
interface-number	Interface number.
detail	Show the detailed information.
N/A	Show the information about all the groups.

Default	N/A
Command mode	Privileged mode.
Usage guidelines	Use this command without any parameters to show group address, interface type, and information about all the multicast groups directly connected to the interface. Information about a specific group is displayed if a group address is added to the command.

Examples

The following example shows information about all the groups:

```
DES-7200# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface Uptime    Expires    Last
Reporter
224.0.1.1        eth2      00:00:09  00:04:17
10.10.0.82
224.0.1.24       eth2      00:00:06  00:04:14
10.10.0.84
224.0.1.40       eth2      00:00:09  00:04:15
10.10.0.91
224.0.1.60       eth2      00:00:05  00:04:15
10.10.0.7
239.255.255.250  eth2      00:00:12  00:04:15
10.10.0.228
239.255.255.254  eth2      00:00:08  00:04:13
10.10.0.84
```

The following example shows detailed information about a specific group:

```
DES-7200# show ip igmp groups 224.1.1.1 detail
Interface       : eth1
Group: 224.1.1.1
Uptime: 00:00:42
Group mode: Include
Last reporter: 192.168.50.111
TIB-A Count: 2
TIB-B Count: 0
Group source list: (R - Remote, M - SSM Mapping)
Source Address Uptime v3 Exp Fwd Flags
192.168.55.55 00:00:42 00:03:38 Yes R
192.168.55.66 00:00:42 00:03:38 Yes R
```

3.2.4 show ip igmp interface

Use this command to show the information of this interface.

Command syntax

show ip igmp [**vrf** *vrf-name*] **interface** [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.
vrf *vrf-name*	Specify the VRF.

	N/A	Show information about all the interfaces.

Default N/A

Command mode User mode or privileged mode.

Examples

The following example shows the information of all the interfaces:

```
DES-7200# show ip igmp interface
Interface vlan1.1 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying device is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds|
IGMP Snooping is globally enabled|
IGMP Snooping is enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
```

3.2.5 show ip igmp ssm-mapping

Use this command to show the **ssm-map** information of the IGMP configuration.

show ip igmp [**vrf** *vrf-name*] **ssm-mapping** [*A.B.C.D*]

Parameter description

Parameter	Description
A.B.C.D	Source address to be mapped
vrf *vrf-name*	Specify the VRF.

Default configuration All the ssm-map information of the IGMP is displayed.

Command mode Privileged mode.

Usage guidelines	If all the parameters are not used, the related configurations are displayed.

Examples	Show the **ssm-map** configuration information:
	`DES-7200# **sh ip igmp ssm-mapping**`
	`SSM Mapping: Enabled`
	`Database : Static mappings configured`
	Show the group information of group 233.3.3.3 to be mapped
	`DES-7200#show ip igmp ssm-mapping 233.3.3.3`
	`Group address: 233.3.3.3`
	`Database : Static`
	`Source list : 192.3.3.3`
	`: 3.3.3.3`

4 MLD Commands

4.1 Configuration Related Commands

4.1.1 clear ipv6 mld group

Use this command to clear the dynamic group member learned by MLD protocol. The dynamic group member refers to the group member record generated by learning the report packets.

clear ipv6 mld group [group-address] [interface-type interface-number]

Parameter description

Parameter	Description
	Remove all group member record learned dynamically.
group-address	IPv6 multicast group address with 128 bits.
interface-type	The associated interface type.
interface-number	The associated interface number.

Default Settings

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

MLD maintains a list of the multicast groups to be added to the host in the directly-connected sub-net. Use the **clear ipv6 mld group** command to remove all dynamic group member record from the MLD group member list.

Examples

The following example shows how to clear all group records:

```
DES-7200# clear ipv6 mld group
```

The following example shows how to clear one group

record:

```
DES-7200# clear ipv6 mld group ff1e::100
```

The following example shows how to clear the record on a specified interface:

```
DES-7200# clear ipv6 mld group ff1e::100 interfa fa0/1
```

Related commands

Command	Description
show ipv6 mld groups	
show ipv6 mld interface	

4.1.2 clear ipv6 mld interface

Use this command to clear all MLD statistical information and the group member records on the interface.

clear ipv6 mld interface interface-type interface-number

Parameter description

Parameter	Description
interface-type	The interface type.
interface-number	The interface id.

Default Settings

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to clear all group information and some packet statistical information learned by LDP on the interface. Those packet statistical information include the number of the received report packets, the number of the done packets and the the number of the group members on the interface.

Examples

```
DES-7200# clear ipv6 mld interface fa 1/1
```

4.1.3 ipv6 mld access-group

Use this command to filter the specific requested group on the interface. Only the report packets in accordance with the corresponding ACL are allowed to be processed. Use the **no** form of this command to disable this function.

ipv6 mld access-group *word*

no ipv6 mld access-group

Parameter description

Parameter	Description
word	The IPv6 ACL name.

Default Settings

No filtering condition has been set.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to filter some groups on the interface and associate with the corresponding ACLs. The correspondent ACL deny report packets will be discarded. This command supports the extended ACL and the source record information of the MLDv2 packets can be filtered.

Caution

The multicast group access control command is associated with the extended ACL. When the received MLD report mesage is (S1,S2,S3…Sn,G), use this command to match and check the (0,G) message using the corresponding ACL. To this end, a (0,G) must be configured for the extended ACL to filter the (S1,S2,S3…Sn,G).

Examples

In the following example, on the interface Eth0/1, the group information carried in the report packets must be in accordance with acl for the normal handling.

```
DES-7200(config)#ipv6 access-list acl
DES-7200(config-ipv6-acl)#permit ipv6 ::/64 ff66::100/64
DES-7200(config-ipv6-acl)#permit ipv6 2222::3333/64 ff66::100/64
DES-7200(config)# interface ethernet 0/1
DES-7200(config-if)# ipv6 mld access-group acl
```

4.1.4 ipv6 mld immediate-leave group-list

Use this command to set the immediate-leave mechanism. With this command configured, the group within the range of group-list, will not send the query packet for the specific group and will remove this group from the group member list immediately after receiving the corresponding done packets. This function is used in the condition that there is only one multicast source that receives the host request on an interface. Use the **no** form of this command to disable this function.

ipv6 mld immediate-leave group-list *word*

no ipv6 mld immediate-leave group-list

Parameter description

Parameter	Description
word	The IPv6 ACL name.

Default Settings

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Without this command configured, when the device receives the MLD leave packets, the request packets for the specific groups will be sent. If there is still no host reply within the response time, the device will remove the corresponding group record from the group member list. The timeout interval is determined by the last member query interval and the MLD robustness variable, and the default value is 2s.

With this command configured, when the device receives the MLD leave packets, it will not send the request packets for the specific groups, but remove the group information immediately, which reduces the leave delay greatly in the condion that there is only one host connecting to the interface.

Examples

The following example shows how to configure the immediate-leave function:

```
DES-7200# configure terminal
DES-7200(config)#ipv6 access-list acl
DES-7200(config-ipv6-acl)#permit ipv6 2222::3333/64
ff66::100/64
```

```
DES-7200(config)# interface ethernet 0/1
DES-7200(config-if)# ipv6 mld immediate-leave group-list
acl
```

Related commands

Command	Description
ipv6 mld last-member-query-interval	

4.1.5 ipv6 mld join-group

Use this command to configure the host action for the switch interface and add the related multicast group to the interface. Use the **no** form of this command to cancel the interface to be added to the multicast group.

ipv6 mld join-group *group-address*

no ipv6 mld join-group *group-address*

Parameter description

Parameter	Description
group-address	The IPv6 non-management multicast group address.

Default Settings

No manual setting is added to the multicast group by default.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to enable the MLD host action on the interface. The interface can not only send the packets initiatively, but also reply to the query packets.

Use this command if it is necessary to join a group member to the interface.

It is worth mentioning that if the group address whose beginning characters are 0xFF*1、0xFF3*, it fails to configure this command. The group address whose beginnning characters are 0xFF*2 fails to form a group.

Examples

The following example shows how to add the host group member:

```
DES-7200# configure terminal
DES-7200(config)# interface fast 0/1
DES-7200(config-if)# ipv6 mld join-group ff55::100
```

4.1.6 ipv6 mld last-member-query-count

last-member-query-count represents that after the interface with MLD enabled receives the done packets, the count number of the times of sending the query packets to the specific group. Use this command to set the last-member-query-count number. Use the **no** form of this command to restore to the default value.

ipv6 mld last-member-query-count *number*

no ipv6 mld last-member-query-count

Parameter description

Parameter	Description
number	The last member query coount number. The valid range is 2-7.

Default Settings

2

Command mode

Interface configuration mode.

Usage guidelines

With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group(multiplied by the value of **mld last-member-query-count**) plus half the reply time.

Examples

The following example shows how to set the last-memer-query-count number as 3:

```
DES-7200# configure terminal
DES-7200(config)# interface ethernet 0/1
DES-7200(config-if)# ipv6 mld last-member-query-count 3
```

4.1.7 ipv6 mld last-member-query-interval

Use this command to set the time interval of sending the quewy packets to the specific group. Use the **no** form of this command to restore it to the default value.

ipv6 mld last-member-query-interval *interval*

no ipv6 mld ast-member-query-interval

Parameter description

Parameter	Description
interval	The valid range is 1-255, in 0.1s.

Default Settings

1s

Command mode

Interface configuration mode.

Usage guidelines

With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group(multiplied by the value of **mld last-member-query-count**) plus half the reply time.

Examples

The following example shows how to set the mld last-member-query-interval as 2s:

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# ipv6 mld last-member-query-interval 20
```

Related commands

Command	Description
ipv6 mld immediate-leave	

4.1.8 ipv6 mld limit(interface configuration mode)

Use this command to enable to learn the max-number of the group member through the MLD protocol. Use the **no** form of this command to disable this function.

ipv6 mld limit *number* [**except** *access-list*]

no ipv6 mld limit

Parameter description

Parameter	Description
number	The maximum number of the group member learned by the MLD.
except *access-list*	(Optional) the ACL beyond the configured mld limit.

Default Settings	1024
Command mode	Interface configuration mode.
Usage guidelines	Use this command to set the max-number of the group members learned through the MLD in the global configuration mode. If the group member number has exceeded the limit, the received report packets later will be discarded and fail to form the group record. If the except list has also been set at the same time, the group member packets, including the packets in the access-list, will be free from the member number limit. This command can also be used in the interface configuration mode. The configurations in two different configuration modes are independent. If the number limit in the global configuration mode is lower than the one in the interface configuration mode, the former configuration takes precedence.

Examples	The following example shows how to set the mld limit as 300:
	`DES-7200(config-if)# ipv6 mld limit 300`
	The following example shows how to set the mld limit as 300, but the configured acl can still learn:
	`DES-7200(config-if)# ipv6 mld limit 300 except acl`

4.1.9 ipv6 mld limit(global configuration mode)

Use this command to enable to learn the max-number of the group member through the MLD protocol. Use the **no** form of this command to disable this function.

ipv6 mld limit *number* [**except** *access-list*]

no ipv6 mld limit *number* [except *access-list*]

Parameter description

Parameter	Description
number	The maximum number of the group member learned by the MLD. The

	valid range is 1-65536.
except *access-list*	(Optional) the ACL beyond the configured mld limit.

Default Settings

Different default values for different products.

Command mode

Global configuration mode.

Usage guidelines

Use this command to set the max-number of the group member learned in the global configuataion mode. The MLD buffering and the packet forwarding are failed for the part of the member packets exceeding the limit. The groups in the except list are free from the number limit.

Examples

The following example shows how to set the mld limit as 300:

```
DES-7200(config)# ipv6 mld limit 300
```

The following example shows how to set the mld limit as 300, and the groups in the acl are free from the limit.

```
DES-7200(config)# ipv6 mld limit 300 except acl
```

4.1.10 ipv6 mld mroute-proxy

Use this command to enable the interface to forward the packets to the correspondent connected interface.

ipv6 mld mroute-proxy interface-type interface-number

no ipv6 mld mroute-proxy

Parameter description

Parameter	Description
interface-type interface-number	The correspondent connected interface.

Default Settings

This function is not configured.

Command mode	Interface configuration mode.
Usage guidelines	After the connected interface has been configured as the proxy-service interface, it can forward the MLD packets sent from other members.
Examples	The following example shows how to set the interface as the mroute-proxy interface: `DES-7200(config-if)# ipv6 mld mroute-proxy fa 0/1`

4.1.11 ipv6 mld proxy-service

Use this command to enable the proxy-service function for the interface connected with the mroute-proxy interface in the downward direction. After configuring this command, the interface becomes the one connected with the mroute-proxy in the upward direction, and associates with and maintains the group information from the interfaces in the downward direction.

ipv6 mld proxy-service

no ipv6 mld proxy-service

Parameter description

Parameter	Description
-	-

Default Settings	No interface is in the proxy-service state.
Command mode	Interface configuration mode.
Usage guidelines	The configurable max-number limit is 32. The number of the interfaces with MLD Proxy enabled is limited by the number multicast interfaces supported device. After receiving the query packet, the proxy-service interface replies according to the member information, which are collected from the mroute-proxy interface and maintained by the proxy-service interface itself. With proxy-service configured, this interface owns the host action rather than the router action. The **ipv6 mld mroute-proxy interface** command configuration on the associated interface in the downward

	direction is removed automatically if the switchport operation is performed on the interfaces.
Examples	The following example shows how to set the interface proxy-service: `DES-7200(config-if)# ipv6 mld proxy-service`

4.1.12 ipv6 mld query-interval

Use this command to set the query interval for the general member. Use the **no** form of this command to restore it to the default value.

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

Parameter description

Parameter	Description
seconds	The query interval for the general member, in seconds. The valid range is 1-18000.

Default Settings	125s
Command mode	Interface configuration mode.
Usage guidelines	The interval of the timer for sending the general query packets can be changed by configuring the query-interval for the general member.

Examples	The following example shows how to set the query-interval for the general member on the interface Ethernet 0:
	`DES-7200(config-if)# ipv6 mld query-interval 120`
	
	The following example shows how to set the query-interval for the general member to the default value on the interface Ethernet 0:
	`DES-7200(config-if)# no ipv6 mld query-interval`

4.1.13 ipv6 mld query-max-response-time

Use this command to set the maximum response time. Use the **no** form of this command to restore it to the default value.

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

Parameter description

Parameter	Description
seconds	The maximum response time, in seconds. The valid range is 1-25.

Default Settings

10s

Command mode

Interface configuration mode.

Usage guidelines

Use this command to control the maximum response time of the host after the device sends the query packets. If there is no response within the maximum response time, MLD will remove the corresponding group from the group member list.

Examples

The following example shows how to set the maximum query response time on the interface gigabitEthernet 0/1:

```
DES-7200(config-if)# ipv6 mld query-max-response-time 20
```

The following example shows how to set the maximum query response time on the interface gigabitEthernet 0/1:

```
DES-7200(config-if)# no ipv6 mld query-max-response-time
```

4.1.14 ipv6 mld querier-timeout

Use this command to set the querier timeout time. Use the **no** form of this command to restore the timeout time of the other querier to the default value.

ipv6 mld querier-timeout *seconds*

no ipv6 mld querier-timeout

Parameter description

Parameter	Description
seconds	Set the querier timeout, in second. The valid range is 60-300.

Default Settings

255s.

Command mode	Interface configuration mode.
Usage guidelines	By default, the **ip mld query interval** value(255s) is the half of the waiting time for the cisco device. If there is no query packet within the interval, the non-querier will become the querier and it will re-elect the querier.

Examples	The following example shows how to set the querier timeout time as 200s:
	`DES-7200(config-if)# ipv6 mld querier-timeout 200`
	The following example shows how to restore the timeout time of the other querier to the default value:
	`DES-7200(config-if)# no ipv6 mld querier-timeout`

4.1.15 ipv6 mld robustness-variable

Use this command to set querier robustness value. Use the **no** form of this command to restore it to the default value.

ipv6 mld robustness-variable *number*

no ipv6 mld robustness-variable

Parameter description

Parameter	Description
number	Set the querier robustness value. The valid range is 2-7.

Default Settings	2.
Command mode	Interface configuration mode.
Usage guidelines	N/A

Examples	The following example shows how to set the querier robustness value as 3:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface ethernet 0`

```
DES-7200(config-if)# ipv6 mld robustness-variable 3
```

4.1.16 ipv6 mld ssm-map enable

Use this command to enable the mld ssm-map function in the global configuration mode.

ipv6 mld ssm-map enable

no ipv6 mld ssm-map enable

Parameter description

Parameter	Description
-	-

Default Settings

Disabled.

Command mode

Global configuration mode.

Usage guidelines

With this command configured, the group information dynamically learned will be added to the related source record forcibly. Usually, this command is set with the **ipv6 mld ssm-map static** command.

Examples

The following example shows how to enable the mld ssm-map function in the global configuratio mode:

```
DES-7200(config)# ipv6 mld ssm-map enable
```

4.1.17 ipv6 mld ssm-map static

Use this command to set the mld ssm-map static mapping source record in the global configuration mode.

ipv6 mld ssm-map static access-list X:X:X:X::X

no ipv6 mld ssm-map static *access-list X:X:X:X::X*

Parameter description

Parameter	Description
access-list	Set the IPv6 ACL name.
X:X:X:X::X	Set the unicast address for the group record mapping.

Default Settings

There is no mapping source address.

Command mode	Global configuration mode.
Usage guidelines	This command is used with the **ipv6 mld ssm-map enable** command. With this command configured, the received mldv1 packets are mapped to the correspondent source record.
Examples	The following example shows how to map all group record of the ACL name te to the source address `4444::1234`: `DES-7200(config)# ipv6 mld ssm-map static te 4444::1234`

4.1.18 ipv6 mld static-group

Use this command to add a group member to the switch interface. Use the **no** form of this command to cancel this function.

ipv6 mld static-group *group-address*

no ipv6 mld static-group *group-address*

Parameter description

Parameter	Description
group-address	Set the IPv6 non-management multicast group address.

Default Settings	By default, no static multicast member manually configured is added.
Command mode	Interface configuration mode.
Usage guidelines	Use this command to add a multicast group to the interface directly. The difference from the join-group is that the packet interaction is not necessay. Use this command when it is necessary to add a group member to the interface. It is worth mentioning that only the **no ipv6 mld static-group** command can be used to delete the group, but not the **clear** command.
Examples	The following example shows how to add the host group member manually: `DES-7200# configure terminal`

```
DES-7200(config)# interface fast 0/1
DES-7200(config-if)# ipv6 mld static-group ff55::3
```

4.1.19 ipv6 mld version

Use this command to set the MLD version number on the interface. Use the **no** form of this command to restore it to the default value.

ipv6 mld version {1 | 2}

no ipv6 mld version

Parameter description

Parameter	Description
{**1** | **2**}	Set the MLD version number.

Default Settings

Version 2.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to control the MLD version number.

Examples

The following example shows how to set the MLD version 1:

```
DES-7200# configure terminal
DES-7200(config)# interface ethernet 0/1
DES-7200(config-if)# ipv6 mld version 1
```

4.2 Showing Related Commands

4.2.1 show ipv6 mld group

Use this command to show the group connected with the switch and the group information learned from the MLD.

show ipv6 mld groups [group-address | interface-type interface-number] [**detail**]

Parameter description

Parameter	Description
group-address	Set the IPv6 multicast group address in 128 bits.

interface-type	Set the interface type.
interface-number	Set the interface number.
detail	Show the information in detail.
	Show all the group information.

Default Settings	N/A.
Command mode	Privileged EXEC mode Interface configuration mode
Usage guidelines	Use this command without the parameters to show the information including the group address, the interface type and the multicast group information. Use this command with a parameter to show the information on a specific group.

Examples

The following example shows all group information:

```
DES-7200# show ipv6 mld groups
MLD Connected Group Membership
Group Address  Interface Uptime Expires  Last Reporter
ff66::1 VLAN1 00:10:57 00:02:16 fe80::2d0:f8ff:fe22:3378
```

The following example shows the detailed information:

```
DES-7200# show ipv6 mld groups detail
Interface:     VLAN 1
Group:         ff66::1
Uptime:        00:10:26
Group mode:    Exclude (Expires: 00:02:47)
Last reporter:  fe80::2d0:f8ff:fe22:3378
Source list is empty
```

4.2.2 show ipv6 mld interface

Use this command to show the configurations on the interface.

show ipv6 mld interface [interface-type interface-number]

Parameter description

Parameter	Description
interface-type	Set the interface type.
interface-number	Set the interface number.
	Show all the interface information.

Default Settings

N/A

Command mode

User EXEC mode or the Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the state information of all interfaces:

```
DES-7200# show ipv6 mld interface
Interface VLAN 2 (Index 4098)
 MLD Enabled, Inactive, Version 2 (default)
 MLD interface limit is 1024
 MLD interface has 0 group-record states
 MLD interface has 1 join-group records
 MLD interface has 0 static-group records
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 10 (1/10s)
 Last member query count is 2
 Group Membership interval is 260
 Robustness Variable is 2
```

4.2.3 show ipv6 mld ssm-mapping

Use this command to show the mapping information of the source address for the group record.

show ipv6 mld ssm-mapping [*group-address*]

Parameter description

Parameter	Description
group-address	Show the source address mapping information for the specific group.
	Show the information for all interfaces.

Default Settings

N/A.

Command mode

User EXEC mode

the Privileged EXEC mode

Usage guidelines

N/A.

Examples

The following example shows the state information of all interfaces:

```
DES-7200# show ipv6 mld ssm-mapping ff66::1234
Group address: ff66::1234
Database    : Static
Source list  : 5555::1234
DES-7200# show ipv6 mld ssm-mapping
SSM Mapping : Enabled
Database    : Static mappings configured
```

5 PIM-DM Commands

5.1 Configuration Related Commands

5.1.1 ip pim dense-mode

Use this command to enable **PIM-DM** on the interface. Use the **no** form of this command to disable the function.

ip pim dense-mode

no ip pim dense-mode

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	Before enabling the PIM-DM, enable the multicast forwarding function in the global configuration mode. Otherwise, the multicast data packet cannot be forwarded even the PIM-DM is enabled. Once the PIM-DM is enabled, the IGMP is enabled automatically on the interface without manual configuration. During the execution of this command, if the prompt "`Failed to enable PIM-DM on <Interface Name>, resource temporarily unavailable, please try again`" appears, re-execute this command. During the execution of this command, if the prompt "`PIM-DM Configure failed! VIF limit exceeded in NSM!!!`" appears, it indicates the allowed configured multicast interface

number exceeds the upper limit of the multicast interfaces. In this case, if it's still necessary to enable the PIM-DM on the interface, delete the unnecessary PIM-DM, PIM-SM or DVMRP interfaces.

It is not recommended to configure different multicat routing protocols on different interfaces of a device.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 0/1
DES-7200(config-if)# ip pim dense-mode
```

5.1.2 ip pim neighbor-filter

Use this command to enable the neighbor filtering on the interface. If the neighbor filtering is set, PIM-DM will not establish the peering relationship with this neighbor or will terminate the established peering relationship with this neighbor once the neighbor is denied by the filtering access list.

The **no** form of this command is used to disable the neighbor filtering function.

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter *access-list*

Parameter description

Parameter	Description
access-list	Access control list supporting numerical ACL in the range of 1 to 99 and name ACL.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

1. When the associated ACL rule is permit, only the neighbor address in ACL can be used as the PIM neighbor of the current interface. When the associated ACL rule is deny, the neighbor address in ACL cannot be used as the PIM neighbor of the current interface.

2. Peering relationship refers to the interaction of

	protocol packets between the PIM neighbors. If the peering relationship with a PIM device is terminated, the neighbor relationship with this device will not be established, and the PIM protocol packets from this device will not be received.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 0/1
DES-7200(config-if)# ip pim neighbor-filter 14
```

5.1.3 ip pim override-interval

Use this command to reconfigure the override-interval of the hello message.The **no** form of this command is used to restore the override-interval to the default value.

ip pim override-interval *interval-milliseconds*

no ip pim override-interval

Parameter description

Parameter	Description
interval-milliseconds	In the range of 1 to 65535 milliseconds.

Default configuration

2500 milliseconds.

Command mode

Interface configuration mode.

Usage guidelines

Configuring the override-interval is to set the pruning veto time for the interface.

Examples

The following example sets the override-interval as 300 milliseconds.

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 0/1
DES-7200(config-if)# ip pim override-interval 3000
```

5.1.4 ip pim propagation-delay

Use this command to reconfigure the propagation-interval of the hello message.The **no** form of this command is used to restore the propagation-interval to the default value.

ip pim propagation-delay *interval-milliseconds*

no ip pim propagation-delay

Parameter description

Parameter	Description
interval-milliseconds	Propagation-interval of the hello message in the range of 1 to 32767 milliseconds.

Default configuration 500 milliseconds.

Command mode Interface configuration mode.

Usage guidelines Configuring the propagation-delay is to set the transmission delay time for the interface.

Examples The following example sets the propagation-delay as 600 milliseconds.

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 0/1
DES-7200(config-if)# ip pim propagation-delay 600
```

5.1.5 ip pim query-interval

Use this command to reconfigure the interval of sending the hello message.The **no** form of this command is used to restore hello interval to the default value.

ip pim query-interval *interval-seconds*

no ip pim query-interval

Parameter description

Parameter	Description
Interval-seconds	Interval of sending the hello message in the range of 1 to 65535 seconds.

Default configuration	30 seconds.
Command mode	Interface configuration mode.
Usage guidelines	If **hello interval** is set, the **hello holdtime** value will be updated to 3.5 times of **hello interval**.

Examples	`DES-7200# configure terminal`
	`DES-7200(config)# interface fastethernet 0/1`
	`DES-7200(config-if)# ip pim query-interval 123`

5.1.6 ip pim state-refresh disable

Use this command to prohibit the interface from processing and forwarding the PIM-DM state refresh messages. The **no** form of this command is used to enable the PIM-DM state refresh function on the interface.

ip pim state-refresh disable

no ip pim state-refresh disable

Parameter description	N/A.
Default	The state refresh message is processed and forwarded by default.
Command mode	Global configuration mode.
Usage guidelines	When the state refresh function is disabled, the PIM-DM state refresh message is not processed and forwarded. The sent Hello message does not contain the status refresh option. Consequently, the SR Cap field will not be processed when the Hello message is received. Generally, it is not recommended to disable the status refresh function because disabling this function may converge the PIM-DM multicast forwarding tree again that has been converged, resulting in unnecessary waste of bandwidth and oscillation of multicast routing table.

Examples	The following example disables the processing of the PIM-DM state refresh message.
	`DES-7200# configure terminal`
	`DES-7200(config)# ip pim state-refresh disable`

5.1.7 ip pim state-refresh origination-interval

Use this command to set the interval of sending the PIM-DM state refresh message. The interval is the seconds elapsed between two state refresh messages. The **no** form of this command restores it to the default value.

ip pim state-refresh origination-interval *interval-seconds*

no ip pim state-refresh origination-interval

Parameter description

Parameter	Description
Interval-seconds	Interval of sending the PIM-DM update message in the range of 1 to 100 in seconds.

Default configuration	60 seconds.
Command mode	Interface configuration mode.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 0/1
DES-7200(config-if)# ip pim state-refresh
origination-interval 65
```

5.2 Showing Related Commands

5.2.1 clear ip pim dense-mode track

Use this command to clear the statistics of PIM-DM packets.

clear ip pim dense-mode track

Parameter description	N/A

Command mode	Privileged mode
Usage guidelines	This command is used to reconfigure the start time of the statistics and clear the PIM packet counter
Examples	`DES-7200# clear ip pim dense-mode track`

Related commands

Command	Description
show ip pim dense-mode track	Show the statistics of the PIM packets.

5.2.2 show ip pim dense-mode interface

Use this command to show the information about the PIM-DM interface.

show ip pim dense-mode interface [*interface-type interface-number*] [**detail**]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and interface ID
detail	Show details of the interface

Default	Privileged/Global configuration/Interface configuration mode
Command mode	User Modeor privileged mode.

Examples

The following example shows the information of the PIM-DM interface:

```
DES-7200# show ip pim dense-mode interface
Address   Interface  VIFIndex  Ver/Mode   Nbr
                                        Mode Count
10.10.10.10 FastEthernet 0/45 3   v2/D        1
50.50.50.50 VLAN4         2      v2/D         1
```

Description of fields in the results:

Field	Description
Address	Primary IP address of the PIM-DM interface
Interface	Name of the PIM-DM interface
VIF Index	VIF ID (ID)
Ver/Mode	PIM version/mode
Nbr Count	Number of neighbors of the PIM-DM interface.

Related commands	Command	Description
	show ip pim dense-mode neighbor	Show the information about the neighbors of the PIM-DM interface.

5.2.3 show ip pim dense-mode mroute

Use this command to show the information about the PIM-DM routing table.

show ip pim dense-mode mroute [*group-or-source-address* [*group-or-source-address*]] [**summary**]

Parameter description	Parameter	Description
	group-or-source-address	Group address or source address
	group-or-source-address	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.
	summary	Show the brief information of routing entries.

Command mode	Privileged/Global configuration/Interface configuration mode

Examples

The following example shows the information about the PIM-Dm routing table:

```
DES-7200# show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
(1.1.1.111, 229.1.1.1)
  MRT lifetime expires in 205 seconds
  RPF Neighbor: 50.50.50.1, Nexthop:50.50.50.1,VLAN 4
  Upstream IF: VLAN 4
    Upstream State: Pruned, PLT:200
    Assert State: NoInfo
  Downstream IF List:
    FastEthernet 0/45:
      Downstream State: NoInfo
      Assert State: Loser, AT:170
```

5.2.4 show ip pim dense-mode neighbor

Use this command to show the information about the PIM-DM neighbors.

show ip pim dense-mode neighbor [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and interface ID.

Command mode

Privileged/Global configuration/Interface configuration mode

Examples

The following example shows the information about the PIM-DM neighbors:

```
DES-7200# show ip pim dense-mode neighbor
Neighbor-Address Interface     Uptime/Expires    Ver
10.10.10.1   FastEthernet 0/45 00:19:29/00:01:21  v2
50.50.50.1   VLAN 4            00:22:09/00:01:39  v2
```

Description of fields in the results:

Field	Description
Neighbor-Address	IP address of the neighbor
Interface	Name of the interface connecting the neighbor

Uptime/Expires	Valid time and aging time of the entry
Ver	PIM version

5.2.5 show ip pim dense-mode nexthop

Use this command to show the information about the PIM-DM next hop.

show ip pim dense-mode nexthop

Parameter description	N/A
Command mode	Privileged/Global configuration/Interface configuration mode

Examples

The following example shows the information about the PIM-Dm next hop:

```
DES-7200# show ip pim dense-mode nexthop
Destination  Nexthop   Nexthop   Nexthop   Metric Pref
               Num       Addr      Interface
1.1.1.111     1       50.50.50.1  VLAN 4    0    1
```

Description of fields in the results:

Field	Description
Destination	Multicast source IP address
Nexthop Num	Number of next hop
Nexthop Addr	IP address of next hop
Nexthop interface	Interface connecting to the of next hop
Metric	Route metric
Pref	Route priority

5.2.6 show ip pim dense-mode track

Use this command to show the statistics of the PIM-DM packets.

show ip pim dense-mode track

Parameter description	N/A

Command mode	Privileged/Global configuration/Interface configuration mode
Usage guidelines	This command is used to show the sent and received PIM packet number since the beginning of the statistics. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the **clear ip pim dense-mode track** every time.

Examples

The following example shows the statistics of the PIM-DM packets:

```
DES-7200# show ip pim dense-mode track
             PIM packet counters
Elapsed time since counters cleared: 00:04:03
                       received    sent
Valid PIMDM packets:       1           8
Hello:                     1           8
Join/Prune:             0          0
Graft:                          0            0
Graft-Ack:                      0            0
Assert:                    0            0
State-Refresh:             0           0
PIM-SM-Register:        0           0
PIM-SM-Register-Stop:     0             0
PIM-SM-BSM:               0               0
PIM-SM-C-RP-ADV:            0            0
Unknown Type:               0
Errors:
Malformed packets:          0
Bad checksums:              0
Unknown PIM version:       0
Send errors:                    0
```

Related commands

Command	Description
clear ip pim dense-mode track	Clear the statistics of the PIM packets.

6 PIM-SM Commands

6.1 Configuration Related Commands

6.1.1 clear ip mroute

clear ip mroute[vrf *vrf-name***]** {* | *group_address [source_address]* }

Parameter description

Parameter	Description
*	Delete all the multicast routing entries.
vrf *vrf-name*	Specify the VRF.
group_address	Delete the multicast routing entries of the specific group.
group_address source_address	Delete the multicast routing entries of the specific group and source IP address.

Default N/A

Command mode Privileged mode

Usage guideline Multicast routing entries can be deleted manually.

Examples

```
DES-7200# clear ip mroute *
DES-7200# clear ip mroute 224.2.2.2
DES-7200# clear ip mroute 224.2.2.2 2.2.2.2
```

6.1.2 clear ip mroute statistics

clear ip mroute statistics[vrf *vrf-name***]** {* | *group_address [source_address]* }

Parameter description

Parameter	Description
*	Delete the statistics of all multicast routing entries.
vrf *vrf-name*	Specify the VRF.
group_address	Delete the statistics of the multicast routing entries of the specific group.
group_address source_address	Delete the statistics of the multicast routing entries of the specific group and source IP address.

Default N/A

Command mode Privileged mode

Usage guideline The statistics of multicast routing entries can be deleted manually.

Examples

```
DES-7200# clear ip mroute statistics *
DES-7200# clear ip mroute statistics 224.2.2.2
DES-7200# clear ip mroute statistics 224.2.2.2 2.2.2.2
```

6.1.3 clear ip pim sparse-mode bsr rp-set

clear ip pim sparse-mode[vrf *vrf-name***] bsr rp-set ***

Parameter description

Parameter	Description
*	Clear all RP-SET.
vrf *vrf-name*	Specify the VRF.

Default N/A

Command mode Privileged mode

Usage guideline All the RP information learnt dynamically can be cleared manually.

Examples

```
DES-7200# clear ip pim sparse-mode bsr rp-set *
```

6.1.4 clear ip pim sparse-mode track

clear ip pim sparse-mode [vrf *vrf-name***]track**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Default N/A

Command mode Privileged mode

Usage guideline This command is used to reconfigure the start time of the statistics and clear the PIM packet counter.

Examples

```
DES-7200# clear ip pim sparse-mode track
```

Related commands

Command	Description
show ip pim sparse-mode track	Show the PIM packet statistics.

6.1.5 ip multicast-routing

ip multicast-routing [vrf *vrf-name***]**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Default Disabled

Command mode Global configuration mode

Usage guideline	This command is mandatory for enabling multicast routing and enabling PIM-SM on an interface. Otherwise, PIM-SM is disabled even though the **ip pim sparse-mode** command is configured.
Examples	`DES-7200(config)# ip multicast-routing`

6.1.6 ip pim accept-bsr list

ip pim [vrf *vrf-name***]accept-bsrr list** *{<1-99>* | *<1300-1999>* | *WORD }*

Parameter description

Parameter	Description
<1-99> | <1300-1999>	IP standard number acl
vrf *vrf-name*	Specify the VRF.
WORD	IP standard name acl

Default	By default, the PIMSM router receives all external BSM packets
Command mode	Global configuration mode
Usage guideline	Use this command to limit the range of the legal BSR.
Examples	`DES-7200# configure terminal` `DES-7200(config)# ip pim accept-bsr list 1`

6.1.7 ip pim accept-crp list

ip pim [vrf *vrf-name***]accept-crp list** {*<100-199>*|*<2000-2699>*|*WORD*}

Parameter description

Parameter	Description
<1-99> | <1300-1999>	IP extension number acl
vrf *vrf-name*	Specify the VRF.
WORD	IP extension name acl

Default	By default, the elected BSR receives all external advertisements of candidate RPs
Command mode	Global configuration mode
Usage guideline	With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.
Examples	`DES-7200 (config)# comfigure terminal` `DES-7200 (config)# ip pim accept-crp list 100`

6.1.8 ip pim accept-crp-with-null-group

ip pim [vrf *vrf-name***]accept-crp-with-null-group**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Default	By default, the BSR does not receive the C-RP-ADV packets whose prefix-count is 0.
Command mode	Global configuration mode
Usage guideline	With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.
Examples	`DES-7200 (config)# configure terminal` `DES-7200 (config)# ip pim accept-crp-with-null-group`

6.1.9 ip pim accept-register list

ip pim [vrf *vrf-name***]accept-register list** *access-lit*

Parameter description

Parameter	Description
~~access-list~~	~~Access control list supporting~~

	numerical ACL in the range of 100 to 199 and 2000 to 2699 and name ACL.
vrf *vrf-name*	Specify the VRF.

Default

There is no restriction on the source IP address pair of register messages on RP.

Command mode

Global configuration mode

Usage guideline

This command is used to restrict the source IP address of register messages on RP.

Examples

```
DES-7200 (config)# ip pim accept-register list 100
DES-7200 (config)# access-list 100 permit ip
192.168.195.0 0.0.0.255 225.1.1.1 0.0.0.255
```

Related commands

Command	Description
access-list	

6.1.10 ip pim bsr-border

ip pim bsr-border

Default

By default, this command is not configured.

Command mode

Interface configuration mode

Usage guideline

To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.

Examples

The following example sets the BSR border on the interface *g 0/3*

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config-if)# ip pim bsr-border
```

6.1.11 ip pim bsr-candidate

ip pim [vrf *vrf-name***]bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority-value*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and number
vrf *vrf-name*	Specify the VRF.
hash-mask-length	(Optional) HASK mask length configured for electing the RP in the range 0 to 32, 10 by default.
priority-value	(Optional) Priority configured for the candidate BSR in the range 0 to 255, 64 by default.

Default N/A

Command mode Global configuration mode

Usage guideline

A PIM-SM domain must contain a unique BootStrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. This packet contains the address and priority of the BSR.

This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IP address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message.

The current device considers itself to be BSR until it

receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IP address).

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim bsr-candidate g 0/3 30 192
```

6.1.12 ip pim dr-priority

ip pim dr-priority *priority-value*

Parameter description

Parameter	Description
priority-value	The larger the value, the higher the priority is. The range is 0 to 4294967294. The default value is 1.

Default

The DR priority is 1 by default.

Command mode

Interface configuration mode

Usage guideline

To select a DR:

- If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices has the same priority, the one of the largest IP address is elected to be the DR.
- If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config-if)# ip pim dr-priority 10000
```

6.1.13 ip pim ignore-rp-set-priority

ip pim [vrf *vrf-name***] ignore-rp-set-priority**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Default

By default, the RP priority of the RP-set is taken into account.

Command mode

Global configuration mode

Usage guideline

This command is used to ignore the priority of the RP corresponding to the multicast group.

Examples

```
DES-7200# configure terminal
DES-7200(config-if)# ip pim ignore-rp-set-priority
```

6.1.14 ip pim jp-timer

ip pim [vrf *vrf-name***] jp-timer** *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	Interval to send the join/prune message in the range 1 to 65535 seconds
vrf *vrf-name*	Specify the VRF.

Default

By default, the Join/Prune message is sent at the interval of 60s.

Command mode

Global configuration mode

Usage guideline

This command is used to set the interval to send the Join/Prune message.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim jp-timer 50
```

6.1.15 ip pim mib

ip pim mib dense-mode

Parameter description	N/A
Default	By default, the MIB of the sparse mode is used.
Command mode	Global configuration mode
Usage guideline	This command is used to use the MIB of the dense mode.
Examples	`DES-7200# configure terminal` `DES-7200(config-if)# ip pim mib dense-mode`

6.1.16 ip pim neighbor-filter

ip pim neighbor-filter *access_list*

Parameter description

Parameter	Description
access_list	Access control list supporting numerical ACL in the range 1 to 99 and name ACL

Default	Disabled
Command mode	Interface configuration mode
Usage guideline	Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config-if)# ip pim neighbor-filter 14
DES-7200(config-if)# exit
DES-7200(config)# access-list 14 deny 192.168.1.5
0.0.0.255
```

Related commands

Command	Description
access-list	

6.1.17 ip pim neighbor-tracking

ip pim neighbor-tracking

Default Enabled

Command mode Interface configuration mode

Usage guideline

Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.

Examples

The following example disables join restraint on the interface.

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config-if)# ip pim neighbor-tracking
```

Related commands

Command	Description
ip pim propagation-delay	

6.1.18 ip pim override-interval

ip pim override-interface *interval-milliseconds*

Parameter description

Parameter	Description
interval-milliseconds	in the range 1 to 65535 milliseconds

Default 2500 milliseconds.

Command mode Interface configuration mode

Usage guideline

Use this command to set the override-interval for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Examples

The following example sets the override-interval as 3000 milliseconds

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config)# ip pim override-interval 3000
```

Related commands

Command	Description
ip pim propagation-delay	

6.1.19 ip pim probe-interval

ip pim [vrf *vrf-name***] probe-interface** *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	in the range 1 to 65535 seconds
vrf *vrf-name*	Specify the VRF.

Default 5 seconds.

Command mode	Global configuration mode
Usage guideline	Use this command to set the registration probe time. The DR can send the null registration message to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet. The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or otherwise the system triggers an alarm.

Examples	The following example sets the probe time as 6 seconds.
	`DES-7200# configure terminal`
	`DES-7200(config)# ip pim probe-interval 6`

Related commands

Command	Description
ip pim register-suppression	

6.1.20 ip pim propagation-delay

ip pim propagation-delay *interval-milliseconds*

Parameter description

Parameter	Description
interval-milliseconds	in the range 1 to 32765 milliseconds

Default	By default, the value of Propagation_delay is 500 milliseconds.
Command mode	Interface configuration mode
Usage guideline	Use this command to set the propagation-delay for the interface. Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Examples

The following example sets the propagation delay as 600 milliseconds.

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config)# ip pim propagation-delay 600
```

Related commands

Command	Description
ip pim override-interval	
Ip pim neighbor-tracking	

6.1.21 ip pim query-interval

ip pim query-interface *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	Interval to send the Hello message in the range 1 to 65535 seconds

Default

By default, the Hello message is sent at the interval of 30s.

Command mode

Interface configuration mode

Usage guideline

Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18752.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config)# ip pim query-interval 123
```

6.1.22 ip pim register-decapsulate-forward

ip pim [vrf *vrf-name***] register-decapsulate-forward**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Command mode

Global configuration mode

Usage guideline

Use this command to implement the decapsulate of the pimsm registration packets with the multicast data packets received on the candidate RP and forward the multicast data packets.

As the decapsulate and forward are performed by the software, it is not recommended to configure this command in the case that many registration packets need to be decapsulated and forwarded, which may cause the cpu busy with this function configured.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim register-decapsulate-forward
```

6.1.23 ip pim register-checksum-wholepkt

ip pim [vrf *vrf-name***] register-checksum-wholepkt** [**group-list** *access-list*]

Parameter description

Parameter	Description
access-list	Access-list: access control list supporting numerical ACL in the range of 100 to 199 and 1300 to 1999 and name ACL. Group-list access-list :all multicast packets use this configuration by default
vrf *vrf-name*	Specify the VRF.

Default

By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message

Command mode

Global configuration mode

Usage guideline	Some vendors' calculate checksum based on the overall registration packets. DES-7200 introduces this function for the compatibility with these vendors.
Examples	DES-7200# **configure terminal** DES-7200(config)#**ip pim register-checksum-wholepkt group-list** *99* DES-7200(config)# a**ccess-list** *99* **permit** *225.1.1.1 0.0.0.255*

Related commands

Command	Description
access-list	

6.1.24 ip pim register-rate-limit

ip pim [vrf *vrf-name***] register-rate-limit** *rate*

Parameter description

Parameter	Description
rate	Maximum number of register packets that can be sent per second, in the range of 1 to 65535
vrf *vrf-name*	Specify the VRF.

Default By default, there is no rate limitation on register messages.

Command mode Global configuration mode

Usage guideline This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim register-rate-limit 3000
```

6.1.25 ip pim register-rp-reachability

ip pim [vrf *vrf-name***] register-rp-reachability**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Default

By default, the RP reachability is not checked before transmission.

Command mode

Global configuration mode

Usage guideline

This command is used to check the RP reachability before transmission. If not, register packets are not transmitted.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim register-rp-reachability
```

6.1.26 ip pim register-source

ip pim [vrf *vrf-name***] register-source** {*source_ip* | *interface-type interface-number*}

Parameter description

Parameter	Description
source_ip	Source IP address of register packets
vrf *vrf-name*	Specify the VRF.
interface-type interface-number	Interface whose IP address is used as the source IP address of register packets

Default

By default, the source IP address of register packets is the IP address of the DR interface connecting the multicast source.

Command mode

Global configuration mode

Usage guideline	This command is used to configure the source IP address of register messages. The source IP address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IP address as the destination IP address of the Register-Stop packet. It is not necessary to enable the PIM.

Examples	`DES-7200# configure terminal`
	`DES-7200(config)# ip pim register-source 192.168.195.80`
	`DES-7200(config)# ip pim register-source g 0/3`

6.1.27 ip pim register-suppression

ip pim [vrf *vrf-name***] register-suppression** *seconds*

Parameter description

Parameter	Description
seconds	Suppression time in the range of 11 to 21843 seconds
vrf *vrf-name*	Specify the VRF.

Default

By default, the register packet suppression time is 60 seconds.

Command mode

Global configuration mode

Usage guideline

Executing this command on the DR will change the register packet suppression time configured. if the **ip pim rp-register-kat** command is not configured, executing this command on RP will modify the period of RP keepalive.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim register-suppression 100
```

6.1.28 ip pim rp-address

ip pim [vrf *vrf-name***] rp-address** *rp-address [access_list]*

Parameter description

Parameter	Description
rp-address	IP address of RP

vrf *vrf-name*	Specify the VRF.
access_list	Access control list supporting numerical ACL in the range 1 to 99 and 1300 to 1999 and name ACL. All multicast groups are supported by default.

Default No IP address is configured for the static RP by default.

Command mode Global configuration mode

Usage guideline

This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that:

- If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence.
- You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once.
- If there are more than one static RP in a multicast group, the one of the highest IP address is used.
- Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted.
- After configuration is performed, the static RP's source IP address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IP address. When you select a RP from a static RP group, the first entry, namely the one wit the largest IP address, will be selected first.
- Deleting a static IP address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP

address.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim rp-address 210.34.0.55 4
DES-7200(config)# access-list 4 permit 255.1.1.1
0.0.0.255
```

Related commands

Command	Description
access-list	

6.1.29 ip pim rp-candidate

ip pim [vrf *vrf-name***] rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *access_list*]

Parameter description

Parameter	Description
interface-type interface-number	Interface
vrf *vrf-name*	Specify the VRF.
priority-value	(Optional) Priority in the range 0 to 255, 192 by default
interval-seconds	(Optional) Interval in the range 0 to 16383 seconds, 60s by default
group_list *access_list*	(Optional) Numberical ACL in the rnage 1 to 99 or name ACL. By default, all multicast groups are permitted.

Default N/A

Command mode Global configuration mode

Usage guideline

In the PIM-SM protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim rp-candidate g 0/3 priority 200
group-list 3 interval 70
DES-7200(config)# access-list 3 permit 255.1.1.1
0.0.0.255
```

Related commands

Command	Description
access-list	

6.1.30 ip pim rp-register-kat

ip pim [vrf *vrf-name***] rp-register-kat** *seconds*

Parameter description

Parameter	Description
seconds	KAT timer time in the range 1 to 65525 seconds
vrf *vrf-name*	Specify the VRF.

Default 210s

Command mode Global configuration mode

Usage guideline This command is used to configure the KAT interval of RP.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim rp-register-kat 250
```

6.1.31 ip pim sparse-mode

ip pim sparse-mode

Parameter description	N/A
Default	Disabled
Command mode	Interface configuration mode
Usage guideline	This command is used to enable PIM-SM on the interface. You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SM. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM. During the execution of this command, if the prompt "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command. During the execution of this command, if the prompt "PIM-SM Configure failed! VIF limit exceeded in NSM!!!" appears, it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SM on the interface, delete the unnecessary PIM-SM, PIM-DM or DVMRP interfaces.

Examples	`DES-7200# configure terminal`
	`DES-7200(config)# interface g 0/3`
	`DES-7200(config-if)# ip pim sparse-mode`

6.1.32 ip pim spt-threshold

ip pim [vrf *vrf-name***] spt-threshold** [**group-list** *access_list*]

Parameter description

Parameter	Description
access_list	(Optional) Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL. By default, all multicast groups are permitted for

	SPT switching.
vrf *vrf-name*	Specify the VRF.

Default By default, SPT switching is disabled.

Command mode Global configuration mode

Usage guideline This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using **group-list**) or all multicast groups (not using **group-list**) .

Examples

```
DES-7200# configure terminal
DES-7200(config)# ip pim spt-threshold
DES-7200(config)# ip pim spt-threshold group-list 12
DES-7200(config)# access-list 12 permit 225.1.1.1
0.0.0.255
```

Related commands

Command	Description
access-list	

6.1.33 ip pim ssm

ip pim [vrf *vrf-name***] ssm** {**default** | **range** *access_list*}

Parameter description

Parameter	Description
default	Multicast groups of 232/8
vrf *vrf-name*	Specify the VRF.
access_list	Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL.

Default Disabled.

Command mode Global configuration mode

Usage guideline	This command is used to enable PIM-SSM (or in some specific multicast groups).

Examples	The following command sets the source-specific multicast of the multicast group range 232/8:
	`DES-7200# configure terminal`
	`DES-7200(config)# ip pim ssm default`
	The following command sets the source-specific multicast with ACL 10.
	`DES-7200(config)# ip pim ssm range 10`
	`DES-7200(config)# access-list 10 permit 232.0.0.1 0.0.0.255`

6.1.34 ip pim triggered-hello-delay

ip pim triggered-hello-delay *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	in the range 1 to 5 seconds

Default	By default, the triggered-hello-delay is 5 seconds.
Command mode	Interface configuration mode
Usage guideline	Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message in random time.

Examples	The following command sets the triggered-hello-delay as 3 seconds
	`DES-7200# configure terminal`
	`DES-7200(config)# interface g 0/3`
	`DES-7200(config-if)# ip pim triggered-hello-delay 3`

6.2 Showing Related Commands

6.2.1 show debugging

show debugging

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command is used to turn on debugging switch.

Examples	`DES-7200 # show debugging`
	`PIM-SM Debugging status:`
	`PIM packet debugging is on.`

6.2.2 show ip pim sparse-mode bsr-router

show ip pim sparse-mode [vrf *vrf-name***] bsr-router**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command is used to show BSR information.

Examples

```
DES-7200# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 192.168.127.1
Uptime:     01d23h14m, BSR Priority: 64, Hash mask
length: 10
Next bootstrap message in 00:00:42
Role: Candidate BSR   Priority: 64, Hash mask length: 10
State: Elected BSR
Candidate RP: 30.30.100.200(GigabitEthernet 0/3)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:32
```

6.2.3 show ip pim sparse-mode interface

show ip pim sparse-mode [vrf *vrf-name***] interface** [*interface-type interface-number* [**detail**]]

Parameter description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all interfaces by default.
vrf *vrf-name*	Specify the VRF.
detail	(Optional) Show the details of an interface.

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command shows the PIM-SM information on the interface.

Examples

```
DES-7200 #show ip pim sparse-mode interface detail
GigabitEthernet 0/3 (vif 2):
  Address 30.30.100.200, DR 30.30.100.200
  Hello period 30 seconds, Next Hello in 13 seconds
  Triggered Hello period 5 seconds
  Neighbors:
   30.30.100.1
```

6.2.4 show ip pim sparse-mode local-members

show ip pim sparse-mode [vrf *vrf-name***] local-member** [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all interfaces by default.
vrf *vrf-name*	Specify the VRF.

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command shows the local IGMP information on the PIM-SM-enabled interface.

Examples

```
DES-7200(config-if)#sh ip pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/3:
(*, 225.1.1.1) : Include
Loopback 1:
GigabitEthernet 0/5:
```

6.2.5 show ip pim sparse-mode mroute

show ip pim sparse-mode [vrf *vrf-name***] mroute** *[group_address|source_address]*

Parameter description

Parameter	Description
group_address	Group IP address in the form of A.B.C.D.
source_address	Source IP address in the form of A.B.C.D
vrf *vrf-name*	Specify the VRF.

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command is used to show route information. Only one group IP address, one source IP address or one group IP address-source IP address pair can be configured at a time. You can also specify no group IP address or source IP address.

6.2.6 show ip pim sparse-mode neighbor

show ip pim sparse-mode [vrf *vrf-name***] neighbor [detail]**

Parameter description

Parameter	Description
detail	(Optional) Show the details of an interface.
vrf *vrf-name*	Specify the VRF.

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command shows the information on neighbors.

Examples

```
DES-7200# show ip pim sparse-mode neighbor detail
Nbr 5.5.5.3 (VLAN 1)
  Expire in 81 seconds
```

6.2.7 show ip pim sparse-mode nexthop

show ip pim sparse-mode [vrf *vrf-name***] nexthop**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command shows the information on the next hop, including interface number, IP address and metric.

6.2.8 show ip pim sparse-mode rp-hash

show ip pim sparse-mode [vrf *vrf-name***] rp-hash** *group-address*

Parameter description

Parameter	Description
group-address	Group address to be resolved

	vrf *vrf-name*	Specify the VRF.

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command shows the information on the RP of the specific group IP address.

Examples

```
DES-7200# show ip pim sparse-mode rp-hash 255.1.1.1
RP: 30.30.100.1
Info source: 30.30.100.1, via bootstrap
```

6.2.9 show ip pim sparse-mode rp mapping

show ip pim sparse-mode [vrf *vrf-name***] rp mapping**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command shows the information on all RPs and the multicast groups they serve.

Examples

```
DES-7200# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 30.30.200.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:00:51, expires: 00:01:39
RP: 30.30.100.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:19:14, expires: 00:01:38
Group(s): 224.0.0.0/4, Static
RP: 100.100.100.100
Uptime: 00:45:35
```

6.2.10 show ip pim sparse-mode track

show ip pim sparse-mode [vrf *vrf-name***] track**

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF.

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline

This command is used to show the sent and received PIM packet number since the beginning of the statistics. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the **clear ip pim sparse-mode track** every time.

Examples

The following example is the output of the **show ip pim sparse-mode track** command

```
DES-7200 # show ip pim sparse-mode track
             PIM packet counters track
Elapsed time since counters cleared: 00:04:03
                        received    sent
Valid PIMSM packets:    0           8
Hello:                    0           8
Join-Prune:           0           0
Register:             0           0
Register-Stop:            0           0
Assert:               0           0
BSM:                      0           0
C-RP-ADV:                 0           0
PIMDM-Graft:            0
PIMDM-Graft-Ack :         0
PIMDM-State-Refresh:      0
Unknown PIM Type:         0
Errors:
Malformed packets:                  0
Bad checksums:                      0
Send errors:                        0
Packets received with unknown PIM version:  0
```

7 PIM-SMv6 Commands

7.1 Configuration Related Commands

7.1.1 clear ipv6 mroute

clear ipv6 mroute {* | *ipv6_group_address* | *ipv6_group_address ipv6_source_address* }

Parameter description

Parameter	Description
*	Delete all the multicast routing entries.
ipv6_group_address	Delete the multicast routing entries of the specific group.
ipv6_group_address source_address	Delete the multicast routing entries of the specific group and source IPV6 address.

Default N/A

Command mode Privileged mode

Usage guideline Multicast routing entries can be deleted manually.

Examples

```
DES-7200# clear ipv6 mroute *
DES-7200# clear ipv6 mroute ff66::6666
DES-7200# clear ipv6 mroute ff66::6666 3333::3333
```

7.1.2 clear ipv6 mroute statistics

clear ipv6 mroute statistics {* | *ipv6_group_address[ipv6_source_address]* }

Parameter description

Parameter	Description
*	Delete the statistics of all multicast routing entries.
ipv6_group_address	Delete the statistics of the multicast routing entries of the specific group.
ipv6_group_address ipv6_source_address	Delete the statistics of the multicast routing entries of the specific group and source IPv6 address.

Default N/A

Command mode Privileged mode

Usage guideline The statistics of multicast routing entries can be deleted manually.

Examples

```
DES-7200# clear ipv6 mroute statistics *
DES-7200# clear ipv6 mroute statistics ff66::6666
DES-7200# clear ipv6 mroute statistics ff66::6666
3333::3333
```

7.1.3 clear ipv6 pim sparse-mode bsr rp-set

clear ipv6 pim sparse-mode bsr rp-set *

Parameter description

Parameter	Description
*	Clear all RP-SET.

Default N/A

Command mode Privileged mode

Usage guideline All the RP information learnt dynamically can be cleared manually.

Examples

```
DES-7200# clear ipv6 pim sparse-mode bsr rp-set *
```

7.1.4 clear ipv6 pim sparse-mode track

clear ipv6 pim sparse-mode track

Default	N/A
Command mode	Privileged mode
Usage guideline	This command is used to reconfigure the start time of the statistics and clear the PIMv6 packet counter
Examples	`DES-7200# clear ipv6 pim sparse-mode track`

Related commands

Command	Description
show ipv6 pim sparse-mode track	

7.1.5 ipv6 multicast-routing

ipv6 multicast-routing

Parameter description	N/A
Default	Disabled
Command mode	Global configuration mode
Usage guideline	This command is mandatory for enabling multicast routing and enabling PIM-SMv6 on an interface. Otherwise, PIM-SMv6 is disabled even though the **ipv6 pim sparse-mode** command is configured.
Examples	`DES-7200(config)# ipv6 multicast-routing`

7.1.6 ipv6 pim accept-bsr list

ipv6 pim accept-bsrr list *WORD*

Parameter description

Parameter	Description
WORD	IPV6 standard name acl

Default By default, the PIM-SMv6 router receives all external BSM packets

Command mode Global configuration mode

Usage guideline Use this command to limit the range of the legal BSR.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ipv6 pim accept-bsr list bsr-list
```

7.1.7 ipv6 pim accept-crp list

ipv6 pim accept-crp list *WORD*

Parameter description

Parameter	Description
WORD	IPV6 extension name acl

Default By default, the elected BSR receives all external advertisements of candidate RPs

Command mode Global configuration mode

Usage guideline With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.

Examples	DES-7200 (config)# **comfigure terminal** DES-7200 (config)# **ipv6 pim accept-crp list** *crp-list*

7.1.8 ipv6 pim accept-crp-with-null-group

ipv6 pim accept-crp-with-null-group

Default	By default, the BSR does not receive the C-RP-ADV packets whose prefix-count is 0.
Command mode	Global configuration mode
Usage guideline	With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.
Examples	DES-7200 (config)# **configure terminal** DES-7200 (config)# **ipv6 pim accept-crp-with-null-group**

7.1.9 ipv6 pim accept-register list

ipv6 pim accept-register list {**list** *ipv6_access-lit* |**route-map** *map-name}*

Parameter description

Parameter	Description
ipv6_access-list	Access control list supporting name ACL.
map-name	Define the routing map rule

Default	There is no restriction on the source IPV6 address pair of register messages on RP.
Command mode	Global configuration mode

Usage guideline	This command is used to restrict the source IPV6 address of register messages on RP. If the unauthorized register source is received, the RP will return the Register-Stop message immediately.

Examples	`DES-7200# configure terminal`
	`DES-7200(config)# ipv6 pim accept-register list register-access-list`
	`DES-7200(config)# ipv6 access-list register-access-list`
	The following example denies the register message of the specified source *fe80::2d0:f8ff:fe22:33ad*
	`DES-7200(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any`

Related commands

Command	Description
ipv6 access-list	

7.1.10 ipv6 pim bsr-border

ipv6 pim bsr-border

Default	By default, this command is not configured.
Command mode	Interface configuration mode
Usage guideline	To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.

Examples	The following example sets the BSR border on the interface *g 0/3*
	`DES-7200# configure terminal`
	`DES-7200(config)# interface g 0/3`
	`DES-7200(config-if)# ipv6 pim bsr-border`

7.1.11 ipv6 pim bsr-candidate

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length*] [*priority-value*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and number
hash-mask-length	(Optional) HASK mask length configured for electing the RP in the range 0 to 128, 126by default.
priority-value	(Optional) Priority configured for the candidate BSR in the range 0 to 255, 64 by default.

Default N/A

Command mode Global configuration mode

Usage guideline

A PIM-SMv6 domain must contain a unique BootStrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. This packet contains the address and priority of the BSR.

This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IPV6 address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message.

The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IPV6 address).

Examples

```
DES-7200# configure terminal
DES-7200(config)# ipv6 pim bsr-candidate g 0/3 30 100
```

7.1.12 ipv6 pim dr-priority

ipv6 pim dr-priority *priority-value*

Parameter description

Parameter	Description
priority-value	The larger the value, the higher the priority is. The range is 0 to 4294967294. The default value is 1.

Default The DR priority is 1 by default.

Command mode Interface configuration mode

Usage guideline

To select a DR:

- If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices has the same priority, the one of the largest IP address is elected to be the DR.
- If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config-if)# ipv6 pim dr-priority 11234
```

7.1.13 ipv6 pim ignore-rp-set-priority

ipv6 pim ignore-rp-set-priority

Parameter description N/A

Default	By default, the RP priority of the RP-set is taken into account.
Command mode	Global configuration mode
Usage guideline	This command is used to ignore the priority of the RP corresponding to the multicast group.
Examples	`DES-7200# configure terminal` `DES-7200(config-if)# ipv6 pim ignore-rp-set-priority`

7.1.14 ipv6 pim jp-timer

ipv6 pim jp-timer *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	Interval to send the join/prune message in the range 1 to 65535 seconds

Default	By default, the Join/Prune message is sent at the interval of 60s.
Command mode	Global configuration mode
Usage guideline	This command is used to set the interval to send the Join/Prune message.
Examples	`DES-7200# configure terminal` `DES-7200(config)# ipv6 pim jp-timer 100`

7.1.15 ipv6 pim neighbor-filter

ipv6 pim neighbor-filter *ipv6_access_list*

Parameter description

Parameter	Description
ipv6_access_list	Access control list supporting name ACL

Default Disabled

Command mode Interface configuration mode

Usage guideline Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config-if)# ipv6 pim neighbor-filter acl
DES-7200(config-if)# exit
DES-7200(config-if)# ipv6 access-list acl
```

The following example denies the neighbor *fe80::2d0:f8ff:fe22:33ad*

```
DES-7200(config-ipv6-acl)#  deny ipv6
fe80::2d0:f8ff:fe22:33ad/128 any
```

Related commands

Command	Description
ipv6_access-list	

7.1.16 ipv6 pim neighbor-tracking

ipv6 pim neighbor-tracking

Default Enabled

Command mode Interface configuration mode

Usage guideline	Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.

Examples	The following example disables join restraint on the interface.
	`DES-7200# configure terminal`
	`DES-7200(config)# interface g 0/3`
	`DES-7200(config-if)# ipv6 pim neighbor-tracking`

Related commands

Command	Description
ipv6 pim propagation-delay	

7.1.17 ipv6 pim override-interval

ipv6 pim override-interface *interval-milliseconds*

Parameter description

Parameter	Description
interval-milliseconds	in the range 1 to 65535 milliseconds

Default	2500 milliseconds.
Command mode	Interface configuration mode

Usage guideline

Use this command to set the override-interval for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Examples

The following example sets the override-interval as 3000 milliseconds

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config)# ipv6 pim override-interval 3000
```

Related commands

Command	Description
ipv6 pim propagation-delay	

7.1.18 ipv6 pim probe-interval

ipv6 pim probe-interface *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	in the range 1 to 65535 seconds

Default

5 seconds.

Command mode

Global configuration mode

Usage guideline

Use this command to set the registration probe time. The DR can send the null registration message to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet.

The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or otherwise the system triggers an alarm.

Examples

The following example sets the probe time as 6 seconds.

```
DES-7200# configure terminal
DES-7200(config)# ipv6 pim probe-interval 6
```

Related commands

Command	Description
ipv6 pim register-suppression	

7.1.19 ipv6 pim propagation-delay

ipv6 pim propagation-delay *interval-milliseconds*

Parameter description

Parameter	Description
interval-milliseconds	in the range 1 to 32765 milliseconds

Default

By default, the value of Propagation_delay is 500 milliseconds.

Command mode

Interface configuration mode

Usage guideline

Use this command to set the propagation-delay for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Examples

The following example sets the propagation delay as 600 milliseconds.

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config)# ipv6 pim propagation-delay 600
```

Related commands

Command	Description
ipv6 pim override-interval	
ipv6 pim neighbor-tracking	

7.1.20 ipv6 pim query-interval

ipv6 pim query-interface *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	Interval to send the Hello message in the range 1 to 65535 seconds

Default By default, the Hello message is sent at the interval of 30s.

Command mode Interface configuration mode

Usage guideline Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18725.

Examples

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/3
DES-7200(config)# ipv6 pim query-interval 60
```

7.1.21 ipv6 pim register-checksum-wholepkt

ipv6 pim register-checksum-wholepkt [**group-list** *ipv6_access-list*]

Parameter description

Parameter	Description
access-list	Access-list: access control list supporting name ACL. Group-list ipv6_access-list :all multicast packets use this configuration by default

Default By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message

Command mode Global configuration mode

Usage guideline

Some vendors' calculate checksum based on the overall registration packets. DES-7200 introduces this function for the compatibility with these vendors.

Examples

```
DES-7200# configure terminal
DES-7200(config)#ipv6 pim register-checksum-wholepkt group-list checksum-access-list
DES-7200(config)# ipv6 access-list 99 checksum-access-list
DES-7200(config-ipv6-acl)# permit ipv6 any ff66::6666/64
```

Related commands

Command	Description
ipv6 access-list	

7.1.22 ipv6 pim register-rate-limit

ipv6 pim register-rate-limit *rate*

Parameter description

Parameter	Description
rate	Maximum number of register packets that can be sent per second, in the range of 1 to 65535

Default

By default, there is no rate limitation on register messages.

Command mode

Global configuration mode

Usage guideline

This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ipv6 pim register-rate-limit 3000
```

7.1.23 ipv6 pim register-rp-reachability

ipv6 pim register-rp-reachability

Parameter description	N/A
Default	By default, the RP reachability is not checked before transmission.
Command mode	Global configuration mode
Usage guideline	This command is used to check the RP reachability before transmission. If not, register packets are not transmitted.
Examples	`DES-7200# configure terminal` `DES-7200(config)# ipv6 pim register-rp-reachability`

7.1.24 ipv6 pim register-source

ipv6 pim register-source {*ipv6_local_address* | *interface-type interface-number*}

Parameter description

Parameter	Description
ipv6_local_address	Source IPV6 address of register packets
interface-type interface-number	Interface whose IPV6 address is used as the source IPV6 address of register packets

Default	By default, the source IPV6 address of register packets is the IPV6 address of the DR interface connecting the multicast source.
Command mode	Global configuration mode

Usage guideline	This command is used to configure the source IPV6 address of register messages. The source IPV6 address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IPV6 address as the destination IPV6 address of the Register-Stop packet. It is not necessary to enable the PIM-SMv6 on the associated interfaces.

Examples	`DES-7200# configure terminal`
	`DES-7200(config)# ipv6 pim register-source 3333::3333`
	`DES-7200(config)# ipv6 pim register-source g 0/3`

7.1.25 ipv6 pim register-suppression

ipv6 pim register-suppression *seconds*

Parameter description

Parameter	Description
suppression	Suppression time in the range of 1 to 65535 seconds

Default	By default, the register packet suppression time is 60 seconds.
Command mode	Global configuration mode
Usage guideline	Executing this command on the DR will change the register packet suppression time configured. if the **ipv6 pim rp-register-kat** command is not configured, executing this command on RP will modify the period of RP keepalive.
Examples	`DES-7200# configure terminal` `DES-7200(config)# ipv6 pim register-suppression 100`

7.1.26 ipv6 pim rp-address

ipv6 pim rp-address *ipv6_rp-address [ipv6_access_list]*

Parameter description

Parameter	Description
ipv6_rp-address	IPV6 address of RP

	ipv6_access_list	Access control list supporting name ACL.

Default No IPV6 address is configured for the static RP by default.

Command mode Global configuration mode

Usage guideline

This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that:

- If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence.
- You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once.
- If there are more than one static RP in a multicast group, the one of the highest IPV6 address is used.
- Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted.
- After configuration is performed, the static RP's source IPV6 address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IPV6 address. When you select a RP from a static RP group, the first entry, namely the one wit the largest IPV6 address, will be selected first.
- Deleting a static IPV6 address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ipv6 pim rp-address 3333::3333 acl
DES-7200(config)# ipv6 pim rp-address 210.34.0.55 4
DES-7200(config)# ipv6 access-list ac
DES-7200(config)# permit ipv6 any ff66::6666/64
```

Related commands

Command	Description
ipv6 access-list	

7.1.27 ipv6 pim rp-candidate

ipv6 pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *ipv6_access_list*]

Parameter description

Parameter	Description
interface-type interface-number	Interface
priority-value	(Optional) Priority in the range 0 to 255, 192 by default
interval-seconds	(Optional) Interval in the range 0 to 16383 seconds, 60s by default
ipv6_access_list	(Optional) name ACL.. By default, all multicast groups are permitted.

Default N/A

Command mode Global configuration mode

Usage guideline

In the PIM-SMv6 protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.

Examples

```
DES-7200# configure terminal
DES-7200(config)# ipv6 pim rp-candidate g 0/3 priority 200
group-list acl interval 40
DES-7200(config)# ipv6 access-list acl
DES-7200(config-ipv6-acl)# permit ipv6  any
ff66::6666/64
```

7.1.28 ipv6 pim rp embedded

ipv6 pim rp embedded [**group-list** *ipv6_acl_name*]

Parameter description

Parameter	Description
ipv6_acl_name	Enable embedded RP for the IPv6 multicast address of specified embedded RP address.

Default

By default, embedded RP is enabled for the IPv6 multicast addresses of all embedded RP addresses.

Command mode

Global configuration mode

Usage guideline

This command is used to enable the embedded RP function explicitly and to enable the embedded RP for the IPv6 multicast address of specified embedded RP address.

Examples

The following example enables the embedded RP for the IPv6 multicast addresses of all embedded RP addresses.

```
DES-7200(config)# ipv6 pim rp embedded
```

Related commands

Command	Description
ipv6 access-list	

7.1.29 ipv6 pim rp-register-kat

ipv6 pim rp-register-kat *seconds*

Parameter description

Parameter	Description
seconds	KAT timer time in the range 1 to

		65525 seconds

Default	210s
Command mode	Global configuration mode
Usage guideline	This command is used to configure the KAT interval of RP.
Examples	`DES-7200# configure terminal` `DES-7200(config)# ipv6 pim rp-register-kat` *250*

7.1.30 ipv6 pim sparse-mode

ipv6 pim sparse-mode

Parameter description	N/A
Default	Disabled
Command mode	Interface configuration mode

Usage guideline	This command is used to enable PIM-SMv6 on the interface. You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SMv6. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM. During the execution of this command, if the prompt "Failed to enable PIM-SMv6 on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command. During the execution of this command, if the prompt "PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!" appears, it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SMv6 on the interface, delete the unnecessary PIM-SMv6,or PIM-DMv6 interfaces. If the interface is of tunnel-type, only 6Over4 configuration tunnel, 6Over GRE tunnel, 6Over4 configuration tunnel and 6Over6 GRE tunnel support the IPv6 multicasting at the moment. The multicasting can also be enabled on other tunnel interfaces which do not support the multicasting, but no error message will be displayed and no multicast packets will be received and forwarded. The multicast tunnel can only be built on the Ethernet interface, the nested tunnel and the multicast data Qos/ACL are not supported.

Examples	`DES-7200# configure terminal`
	`DES-7200(config)# interface g 0/3`
	`DES-7200(config-if)# ipv6 pim sparse-mode`

7.1.31 ipv6 pim spt-threshold

ipv6 pim spt-threshold [**group-list** *ipv6_access_list*]

Parameter description

Parameter	Description
ipv6_access_list	(Optional) supporting name ACL.. By default, all multicast groups are permitted for SPT switching.

Default	By default, SPT switching is disabled.
Command mode	Global configuration mode
Usage guideline	This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using **group-list**) or all multicast groups (not using **group-list**) .

Examples	`DES-7200(config)# ipv6 pim spt-threshold acl`
	`DES-7200(config)# ipv6 access-list acl`
	`DES-7200(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad /128 ff66::6666/64`

Related commands

Command	Description
ipv6 access-list	

7.1.32 ipv6 pim ssm

ipv6 pim ssm {**default** | **range** *ipv6_access_list*}

Parameter description

Parameter	Description
default	Group in the range of FF3x::/32
range ipv6_access_list	Supporting name ACL.

Default	Disabled.
Command mode	Global configuration mode
Usage guideline	This command is used to enable PIM-SSMv6 (or in some specific multicast groups).

Examples

The following command sets the source-specific multicast of the multicast group range acl:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 pim ssm range acl
```

The following command uses SSM for the source address fe80::2d0:f8ff:fe22:33ad, group range of ff32::3333/64 .

```
DES-7200(config-ipv6-acl)# permit ipv6
fe80::2d0:f8ff:fe22:33ad /128  ff32::3333/64
```

Related commands

Command	Description
ipv6 access-list	

7.1.33 ipv6 pim static-rp-preferred

ipv6 pim static-rp-preferred

Default

By default, the priority of the RP elected through BSR mechanism is high than the one configured statically.

Command mode

Interface configuration mode

Usage guideline

With this command configured, the priority of the static RP is higher than the one elected through the BSR mechanism.

Examples

The following command configures the the priority of the static RP is higher than the one elected through the BSR mechanism.

```
DES-7200# configure terminal
DES-7200(config-if)# ipv6 pim static-rp-preferred
```

7.1.34 ipv6 pim triggered-hello-delay

ipv6 pim triggered-hello-delay *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	in the range 1 to 5 seconds

Default	By default, the triggered-hello-delay is 5 seconds.
Command mode	Interface configuration mode
Usage guideline	Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message at the random time.

Examples	The following command sets the triggered-hello-delay as 3 seconds
	`DES-7200# configure terminal`
	`DES-7200(config)# interface g 0/3`
	`DES-7200(config-if)# ipv6 pim triggered-hello-delay 3`

7.2 Showing Related Commands

7.2.1 show debugging

show debugging

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command is used to turn on debugging switch.

Examples	`DES-7200 # show debugging`
	`PIM-SM Debugging status:`
	`PIM packet debugging is on.`

7.2.2 show ipv6 pim sparse-mode bsr-router

show ipv6 pim sparse-mode bsr-router

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command is used to show BSR information.
Examples	DES-7200# **show ipv6 pim sparse-mode bsr-router** PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 3333::8888 Uptime:00:03:31, BSR Priority: 64, Hash mask length: 126 Next bootstrap message in 00:00:47 Role: Candidate BSR Priority: 64, Hash mask length: 126 State: Elected BSR Candidate RP: 3333::8888(GigabitEthernet 0/5) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:37

7.2.3 show ipv6 pim sparse-mode interface

show ipv6 pim sparse-mode interface [*interface-type interface-number* [**detail**]]

Parameter description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all interfaces by default.
detail	(Optional) Show the details of an interface.

Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command shows the PIM-SMv6 information on the interface.

Examples

```
DES-7200 #show ipv6 pim sparse-mode interface detail
GigabitEthernet 0/5 (vif 1):
Address          fe80::2d0:f8ff:fe22:33ad,          DR
fe80::2d0:f8ff:fe22:34b3
Hello period 30 seconds, Next Hello in 6 seconds
Triggered Hello period 5 seconds
Secondary addresses:
  3333::8888
  4444::4444
 Neighbors:
  fe80::2d0:f8ff:fe22:34b3
```

7.2.4 show ipv6 pim sparse-mode local-members

show ipv6 pim sparse-mode local-member [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all interfaces by default.

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline

This command shows the local MLD information on the PIM-SMv6-enabled interface.

Examples

```
DES-7200 (config-if)#show ipv6 pim sparse-mode
local-members
PIM Local membership information
GigabitEthernet 0/5:
  (*, ff66::6666) : Include
```

7.2.5 show ipv6 pim sparse-mode mroute

show ipv6 pim sparse-mode mroute [*group-or-source-address* [*group-or-source-address*]]

Parameter description

Parameter	Description
group-or-source-address	Group address or source address

group-or-source-address	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline

This command is used to show route information. Only one group IPv6 address, one source IPv6 address or one group IPv6 address-source IPv6 address pair can be configured at a time. You can also specify no group IP address or source IPv6 address.

7.2.6 show ipv6 pim sparse-mode neighbor

show ipv6 pim sparse-mode neighbor [detail]

Parameter description

Parameter	Description
detail	(Optional) Show the details of an interface.

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline

This command shows the information on neighbors.

Examples

```
DES-7200# show ipv6 pim sparse-mode neighbor detail
Nbr fe80::2d0:f8ff:fe22:34b3 (GigabitEthernet 0/5)
 Expires in 86 seconds
  Secondary addresses:
   6666::6666
```

7.2.7 show ipv6 pim sparse-mode nexthop

show ipv6 pim sparse-mode nexthop

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command shows the information on the next hop, including interface number, IP address and metric.

7.2.8 show ipv6 pim sparse-mode rp-hash

show ipv6 pim sparse-mode rp-hash *ipv6_group-address*

Parameter description

Parameter	Description
ipv6_group-address	Group address to be resolved

Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command shows the information on the RP of the specific group IPv6 address.

Examples

```
DES-7200# show ipv6 pim sparse-mode rp-hash ff66::6666
RP: 3333::8888
Info source: 3333::8888, via bootstrap
PIMv2 Hash Value 126
RP 3333::8888, via bootstrap, priority 192, hash value 1468234650
```

7.2.9 show ipv6 pim sparse-mode rp mapping

show ipv6 pim sparse-mode rp mapping

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline	This command shows the information on all RPs and the multicast groups they serve.

Examples

```
DES-7200# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 3333::1
    Info source: 3333::1, via bootstrap, priority 192
         Uptime: 00:12:40, expires: 00:01:50
```

7.2.10 show ipv6 pim sparse-mode track

show ipv6 pim sparse-mode track

Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command is used to show the sent and received PIM packet number since the beginning of the statistics. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIMv6 packet counter is cleared on calling the **clear ipv6 pim sparse-mode track** every time.

Examples

The following example is the output of the **show ipv6 pim sparse-mode track** command

```
DES-7200# show ipv6 pim sparse-mode track
PIMv6 packet counters track
Elapsed time since counters cleared: 00:04:03
                           received     sent
Valid PIMSMv6 packets:     0                8
Hello:                          0                8
Join-Prune:                0                0
Register:                  0                0
Register-Stop:             0                0
Assert:                         0                0
BSM:                       0                0
C-RP-ADV:                  0                0
PIMDMv6-Graft:             0
PIMDMv6-Graft-Ack:              0
PIMDMv6-State-Refresh:          0
Unknown PIMv6 Type:        0
Errors:
Malformed packets:                               0
Bad checksums:
    0
Send errors:
    0
Packets received with unknown PIMv6 version:    0
```

8 IGMP Snooping Commands

8.1 Configuration Related Commands

8.1.1 deny

To deny the forwarding of the multicast streams in the range specified by the profile, execute the **deny** configuration command in the profile configuration mode.

deny

Parameter description	N/A
Default	The forwarding of the multicast streams in the range specified by the profile is denied.
Command mode	Profile configuration mode.
Usage guidelines	First, configure the multicast range using the **range** command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Examples	The following is an example of deny the forwarding of the multicast stream 224.2.2.2:
	`DES-7200(config)# ip igmp profile 1`
	`DES-7200(config-profile)# range 224.2.2.2`
	`DES-7200(config-profile)# deny`

Related commands

Command	Description
ip igmp	Create a profile.

profile	
range	Configure the multicast address range.

8.1.2 ip igmp profile

This is a mode navigation command. Use this command to select a profile and enter the IGMP profile configuration mode.

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

Parameter description

Parameter	Description
profile-number	Profile number, in the range from 1 to 65535

Default N/A.

Command mode Global configuration mode.

Usage guidelines The profile must be applied to the specified interface in order to make the profile take effect.

Examples

The following is an example of creating a profile numbered 1 and entering the profile configuration mode.

```
DES-7200(config)# ip igmp profile 1
DES-7200(config-profile)#
```

Related commands

Command	Description
range	Configure the multicast address range.

8.1.3 ip igmp snooping dyn-mr-aging-time

To configure the aging time of the routing interface that the switch learns dynamically, execute the **ip igmp snooping dyn-mr-aging-time** command .

ip igmp snooping dyn-mr-aging-time *time*

no ip igmp snooping dyn-mr-aging-time

Parameter

Parameter	Description

description	*time*	Aging time of the routing interface that the switch learns dynamically

Default configuration	300s.
Command mode	Global configuration mode.
Usage guidelines	When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.
Examples	Set the aging time of the routing interface that the switch learns dynamically to 100 s: `DES-7200(config)# ip igmp snooping dyn-mr-aging-time 100`

Related commands

Command	Function
ip igmp snooping	Enable IGMP snooping.

8.1.4 ip igmp snooping fast-leave enable

To enable the fast leave function, execute the **ip igmp snooping fast-leave enable** command in the global configuration mode. The **no** form of this command is used to disable the function.

ip igmp snooping fast-leave enable

no ip igmp snooping fast-leave enable

Parameter description

Parameter	Description
N/A	

Default configuration	Disabled.
Command mode	Global configuration mode.

Usage guidelines

After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message.

Examples

The following example shows how to enable the fast leave function on the switch:

```
DES-7200(config)# ip igmp snooping fast-leave
```

Related commands

Command	Function
N/A	

8.1.5 ip igmp snooping filter

To configure a port to receive a specific set of multicast streams, execute the **ip igmp snooping filter** command in the interface configuration mode to associate the port to a specific profile. The **no** form of this command is used to delete the associated profile.

ip igmp snooping filter *profile-number*

no ip igmp snooping filter *profile-number*

Parameter description

Parameter	Description
profile-number	Profile number

Default N/A.

Command mode Interface configuration mode.

Usage guidelines A specific profile must be created before association.

Examples

The following example demonstrates how to associate profile 1 to a megabit port 0/1:

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip igmp snooping filter 1
```

Related commands	

Command	Description
ip igmp profile	Create a profile.

8.1.6 ip igmp snooping ivgl

To enable IGMP snooping and enter the IVGL mode, execute the **ip igmp snooping ivgl** command in the global configuration mode. The **no** form of this command is used to disable IGMP snooping.

ip igmp snooping ivgl

no ip igmp snooping

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	After this mode is set, for multicast frames with the same multicast address yet in different VLANs, the **IGMP snooping** function handles only the same group as that in the multicast address table (GDA), other multicast frames are forwarded.
Examples	The following example demonstrates how to enable IGMP snooping and enter the IVGL mode: `DES-7200(config)# ip igmp snooping ivgl`

Related commands

Command	Description
ip igmp snooping svgl	Enable igmp snooping and enter the SVGL mode.
ip igmp snooping ivgl-svgl	Enable igmp snooping and enter the hybrid mode.

8.1.7 ip igmp snooping ivgl-svgl

To enable IGMP snooping and enter the ivgl-svgl mode, execute the **ip igmp snooping ivgl-svgl** command in the global configuration mode. The **no** form of this command is used to disable IGMP snooping.

ip igmp snooping ivgl-svgl

no ip igmp snooping

Parameter description	N/A.
Default	Disabed.
Command mode	Global configuration mode.
Usage guidelines	After this mode is set, IVGL and SVGL coexist.
Examples	The following example demonstrates how to enable IGMP snooping and enter the ivgl-svgl mode on the device: `DES-7200(config)# ip igmp snooping ivgl-svgl`

Related commands

Command	Description
ip igmp snooping svgl	Enable igmp snooping and enter the SVGL mode.
ip igmp snooping ivgl	Enable igmp snooping and enter the IVGL mode.

8.1.8 ip igmp snooping limit-ipmc

To add a multicast source IP address check entry, execute the **ip igmp snooping limit-ipmc** command in the global configuration mode. The **no** form of this command is used to delete a source IP checklist entry.

ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

no ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

Parameter description

Parameter	Description
Vid	VLAN ID of the source IP address check entry
Gaddress	Multicast address
Saddress	Multicast source IP address (multicast server)

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	The source IP address check function must be enabled before an entry can be added.
Examples	The following is an example of adding an entry to the multicast source IP address check table. `DES-7200(config)# ip igmp snooping limit-ipmc vlan 1 address 224.0.0.1 server 192.168.4.243`

Related commands

Command	Description
ip igmp snooping source-check default-server	Configure a default source IP address while enabling the IP check function.

8.1.9 ip igmp snooping max-groups

To configure the maximum number of groups that can be added dynamically to this interface, execute the **ip igmp snooping max-groups** command in the interface configuration mode. The **no** form of this command is used to remove the configuration.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

Parameter description

Parameter	Description
number	The parameter ranges 0 to 4294967294.

Default	N/A.
Command mode	Interface configuration mode.
Usage guidelines	If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this

	interface is beyond the range.

Examples	The following example shows how to configure the maximum number of multicast groups to 100 on the megabit interface 0/1:
	`DES-7200(config)# interface fastEthernet 0/1`
	`DES-7200(config-if)# ip igmp snooping max-group 100`

Related commands

Command	Description
ip igmp snooping filter	Filter multicast groups that pass through a port.

8.1.10 ip igmp snooping mrouter learn pim-dvmrp

To configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface, execute the **ip igmp snooping mrouter learn** command in the global configuration mode. The **no** form of this command is used to disable the dynamic learning.

ip igmp snooping mrouter learn pim-dvmrp

no ip igmp snooping mrouter learn pim-dvmrp

Default	Enabled
Command mode	Global configuration mode.
Usage guidelines	Routing interface is a port through which a multicast device is directly connected to a multicast neighbouring device By default, the dynamic routing interface learning function is enabled. You can use the **no** form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled. When the source port check function is enabled, only the multicast flow enters from the routing interface is legal and it is forwarded to the registered interface by the multicast equipment, the multicast flow from the non routing interface is considered to be the illegal and is

	discarded. With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.
Examples	The following example demonstrates how to enable the dynamic routing interface learning function on the equipment: `DES-7200(config)# ip igmp snooping mrouter learn pim-dvmrp`

Related commands	**Command**	**Description**
	ip igmp snooping vlan mrouter learn pim-dvmrp	Enable the dynamic routing interface learning function on the multicast routing port.

8.1.11 ip igmp snooping preview

Allow the user to preview the specific multicast streams when the user doesn't have access to such multicast streams. Use **no** form of this command to disable multicast preview.

ip igmp snooping preview *profile-number*

no ip igmp snooping preview

Parameter description	**Parameter**	**Description**
	profile-number	Profile number (1-1024)

Default	No default value
Command mode	Global configuration mode.
Usage guidelines	Apply the IGMP Profile to a multicast preview function. When the user doesn't have access to the multicast streams (namely the user might be filtered by IGMP Snooping filter), it can allow the user to preview partial contents. This function shall be used in conjunction with IGMP Snooping filter or multicast control in order to realize effective multicast preview.

Examples

The following example associates the profile 1 to the 100M port 0/1 and associates multicast preview with profile 2:

```
DES-7200(config)# ip igmp snooping preview 2
DES-7200(config-if)# int fa 0/1
DES-7200(config-if)# ip igmp snooping filter 1
```

Related commands

Command	Description
ip igmp profile	Create a profile

8.1.12 ip igmp snooping preview interval

Use this command to configure the interval that allows the user to preview the specific multicast streams when the user doesn't have access to such multicast streams. Use **no** form of this command to restore the preview interval to the default value.

ip igmp snooping preview interval *num*

no ip igmp snooping preview interval

Parameter description

Parameter	Description
num	Preview interval (1-300); default: 60 seconds.

Default

The default value is 60 seconds.

Command mode

Global configuration mode.

Usage guidelines

NA

Examples

The following example sets the multicast preview interval as 100 seconds on the 100M port of 0/1:

```
DES-7200(config)# ip igmp snooping preview interval 100
```

	Command	Description
Related commands	**ip igmp snooping preview**	Enable the multicast preview.

8.1.13 ip igmp snooping querier

To enable the IGMP querier function, execute "**ip igmp snooping querier**" global configuration command. Use **no** form of this command to disable IGMP querier in all VLANs and disable the global configurations.

ip igmp snooping querier

no ip igmp snooping querier

	Parameter	Description
Parameter description	-	-

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to effect this command. If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.
Examples	The following example enables the IGMP querier function on the device: `DES-7200(config)# ip igmp snooping querier`

	Command	Description
Related commands	**ip igmp snooping vlan querier**	Enable the querier function in VLAN

8.1.14 ip igmp snooping querier address

To enable the IGMP querier, you also need to specify a source IP address for query packets. Execute the global configuration command of "**ip igmp snooping querier address**". Use **no** form of this command to remove the source IP address configured.

ip igmp snooping querier address *a.b.c.d*

no ip igmp snooping querier address

Parameter description

Parameter	Description
a.b.c.d	Source IP address of the query packets.

Default

No source IP address is specified

Command mode

Global configuration mode.

Usage guidelines

After enabling IGMP querier, you also need to configure a source IP address for query packets, so that the device can send packets normally.

If no source IP address is specified in the VLAN needing to send packets, the device will verify whether the source IP address is specified globally. The device can only send query packets after finding the source IP configured, or else the querier function won't take effect.

If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.

Examples

The following example specifies the source IP of query packets on the device:

```
DES-7200(config)# ip igmp snooping querier address 1.1.1.1
```

Related

Command	Description

commands	**ip igmp snooping vlan querier address**	Enable the source IP check in VLAN

8.1.15 ip igmp snooping querier max-response-time

To configure the maximum response time advertised in query packets, execute the global configuration command of "**ip igmp snooping querier max-response-time**". Use **no** form of this command to restore to the default value.

ip igmp snooping querier max-response-time *num*

no ip igmp snooping querier max-response-time

	Parameter	Description
Parameter description	*num*	Maximum response time (1-25); unit: second; default: 10

Default	Default value
Command mode	Global configuration mode.
Usage guidelines	Configure this command to specify the maximum response time to query packets. By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.
Examples	The following example specifies the maximum response time to query packets on the device: `DES-7200(config)# ip igmp snooping querier max-response-time 15`

	Command	Description
Related		

commands	**ip igmp snooping vlan querier max-response-time**	Configure the maximum response time to query packets in VLAN

8.1.16 ip igmp snooping querier query-interval

To specify the interval for IGMP querier to send query packets, execute the global configuration command of "**ip igmp snooping querier query-interval**". Use **no** form of this command to restore the query interval to the default value.

ip igmp snooping querier query-interval *num*

no ip igmp snooping querier query-interval

Parameter description

Parameter	Description
num	Query interval (1-18000); unit: second; default: 60 seconds

Default

Default value

Command mode

Global configuration mode.

Usage guidelines

After globally enabling IGMP querier, the timer will be enabled for sending query packets periodically. The aging time of the timer is the query interval. Configure this command to change the query interval.

If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Examples

The following example configures the query interval on the device:

```
DES-7200(config)# ip igmp snooping querier query-interval 100
```

Related

Command	Description

commands	**ip igmp snooping vlan querier query-interval**	Configure the query interval in VLAN

8.1.17 ip igmp snooping querier timer expiry

To specify the expiration timer for non-querier, execute the global configuration command of "**ip igmp snooping querier timer expiry**". Use **no** form of this command to restore to the default value.

ip igmp snooping querier timer expiry *num*

no ip igmp snooping querier timer expiry

	Parameter	Description
Parameter description	*num*	Non-querier expiration timer (60-300); unit: second; default: 125 seconds

Default	Default value
Command mode	Global configuration mode.
Usage guidelines	After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier. If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.
Examples	The following example configures the non-querier expiration timer on the device: `DES-7200(config)# ip igmp snooping querier timer expiry 60`

Related	Command	Description

commands	**ip igmp snooping vlan querier timer expiry**	Configure querier expiration timer in VLAN

8.1.18 ip igmp snooping querier version

Currently, the IGMP Snooping querier supports IGMPv1 and IGMPv2. To specify the version, execute the global configuration command of "**ip igmp snooping querier version**". Use **no** form of this command to restore to the default setting.

ip igmp snooping querier version *num*

no ip igmp snooping querier

	Parameter	Description
Parameter description	*num*	IGMP version number (1-2). Default value: 2.

Default	IGMPv2
Command mode	Global configuration mode.
Usage guidelines	If the IGMP querier version number has been configured in the corresponding VLAN, the value specified in VLAN will be used first.
Examples	The following example configures IGMP querier version on the device: `DES-7200(config)# ip igmp snooping querier version 1`

	Command	Description
Related commands	-	-

8.1.19 ip igmp snooping query-max-response-time

This command specifies the time for the switch to wait for the member join message after receiving the **query** message. If the switch does not receive the

member join message within the specified time, it considers that the member has left and then deletes the member.

ip igmp snooping query-max-response-time *time*

no ip igmp snooping query-max-resposne-time

Parameter description

Parameter	Description
time	The aging time of the routing inerface that the switch learns dynamically.

Default configuration

10s.

Command mode

Global configuration mode.

Usage guidelines

You can specify the time for the switch to wait for the member join message after receiving the **query** message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member. This command lets you adjust the waiting time after receiving the **query** message.

Examples

Set the aging time of the routing interface that the switch learns dynamically to 100s.

```
DES-7200(config)# ip igmp snooping query-max-response-time 100
```

Related commands

Command	Function
ip igmp snooping	Configure a multicast routing interface.

8.1.20 ip igmp snooping source-check default-server

The source IP address check is used to permit one or several IPMC flows from the server of the specified IP address.

To configure the source IP address check function of IGMP snooping, execute the **ip igmp snooping source-check default-server** command in the global

configuration mode. The **no** form of this command is used to disable the source IP address check function.

ip igmp snooping source-check default-server *address*

no ip igmp snooping souce-check

Parameter description

Parameter	Description
address	Default multicast source IP address (IP address of the default multicast server)

Default Disabled.

Command mode Global configuration mode.

Usage guidelines The source IP address check function takes effect globally. Once it is enabled, only the IPMC streams from the specified IP address are permitted. The device allows users to configure the source IP address of all IPMC streams, called default multicast server. The default server must be set as long as the source IP address check function is enabled.

Examples The following example shows how to enable the multicast source IP address check function and configure a default source IP address.

```
DES-7200(config)# ip igmp snooping source-check
default-server 192.168.4.243
```

Related commands

Command	Description
Ip igmp snooping limit-ipmc vlan server	Add an entry to the source IP check table.

8.1.21 ip igmp snooping source-check port

The source port check function is used to permit one or several IPMC flows from the mroute port.To configure the source port check function of IGMP snooping, execute the **ip igmp snooping source-check port** command in the global configuration mode. The no form of this command is used to disable the source port check function.

ip igmp snooping source-check port

no ip igmp snooping source-check port

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The source port check function takes effect globally. Once it is enabled, only the IPMC streams from the specified port are permitted.
Examples	The following example shows how to enable the source port check function of IGMP snooping. `DES-7200(config)# ip igmp snooping source-check port`

Related commands

Command	Description
Ip igmp snooping source-check default-server	Enable the multicast source IP address check function.

8.1.22 ip igmp snooping suppression enable

To enable IGMP snooping suppression, execute the **ip igmp snooping suppression enable** command in the global configuration mode.The **no** form of this command is used to disable IGMP snooping suppression..

ip igmp snooping suppression enable

no ip igmp snooping suppression enable

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.

Usage guidelines	After you execute this command to enable the suppression function, the switch begins to suppress the **IGMP v1/v2** report messages.
Examples	The following example shows how to enable IGMP snooping suppression on the device: `DES-7200(config)# ip igmp snooping suppression`
Related commands	N/A

8.1.23 ip igmp snooping svgl

To enable IGMP snooping and enter the SVGL mode, execute the **ip igmp snooping svgl** command in the global configuration mode. The **no** form of this command is used to disable IGMP snooping.

ip igmp snooping svgl

no ip igmp snooping

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The SVGL works only when the multicast IP address range is configured.
Examples	The following example demonstrates how to enable IGMP snooping and enter the SVGL mode: `DES-7200(config)# ip igmp snooping svgl`

Related commands

Command	Description
ip igmp snooping ivgl	Enable igmp snooping and

	enter the IVGL mode.
ip igmp snooping ivgl-svgl	Enable igmp snooping and enter the hybrid mode

8.1.24 ip igmp snooping svgl profile

To specify the multicast group address range applied in the SVGL/IVGL-SVGL mode, execute the **ip igmp snooping profile** *profile-number* command in the global configuration mode. Use the **no ip igmp snooping profile** command to cancel the association.

ip igmp snooping profile *profile-number*

no ip igmp snooping profile

Parameter description

Parameter	Description
profile-number	Profile number, in the range of 1-65535.

Default No profile is associated.

Command mode Global configuration mode.

Usage guidelines

When the IGMP Snooping works in the SVGL or IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode. That is to say, the member ports of the multicast forwarding entry can be forwarded across the VLANs while the member ports of the multicast forwarding entry in the other multicast address range must belong to the same VLAN. By default, no profile is associated.

Examples

```
DES-7200(config)# ip igmp snooping svgl profile 1
```

Related commands

Command	Description
ip igmp snooping ivgl	Enable igmp snooping and enter the IVGL mode.
ip igmp snooping ivgl-svgl	Enable igmp snooping and enter the hybrid mode

8.1.25 ip igmp snooping svgl subvlan

To specify the subvlan of multicast VLAN, execute the global configuration command of "**ip igmp snooping svgl subvlan**". Use **no** form of this command to remove this configuration.

ip igmp snooping svgl subvlan [*vid-range*]

no ip igmp snooping svgl subvlan [*vid-range*]

Parameter description

Parameter	Description
vid-range	VLAN ID or range of VLAN ID

Default

By default, no subvlan is specified for svgl, and all VLANs serve as its subvlans.

Command mode

Global configuration mode.

Usage guidelines

This command only takes effect in SVGL or IVGL-SVGL mode.

Examples

The following example configures the device operating in igmp snooping svgl mode to associate VLAN 2, 5, 6 and 7:

```
DES-7200(config)# ip igmp snooping svgl vlan 2,5-7
```

Related commands

Command	Description
ip igmp snooping svgl	Enable the igmp snooping and configure the svgl mode.
ip igmp snooping ivgl-svgl	Enable the igmp snooping and configure the IVGL-SVGL mode.
ip igmp snooping svgl vlan	Configure the primary VLAN of SVGL mode.

8.1.26 ip igmp snooping svgl vlan

To specify the vlan as the shared vlan in the SVGL mode, execute the **ip igmp snooping svgl vlan** command in the global configuration mode. The **no** form of this command restores the Shared VLAN to vlan 1..

ip igmp snooping svgl vlan *vid*

no ip igmp snooping svgl vlan

Parameter description

Parameter	Description
vid	VLAN ID.

Default By default , the shared vlan is vlan1.

Command mode Global configuration mode.

Usage guidelines This command only works in the SVGL or IVGL-SVGL mode.

Examples The following example specifies the vlan2 as the shared vlan

```
DES-7200(config)# ip igmp snooping svgl vlan 2
```

Related commands

Command	Description
ip igmp snooping svgl	Enable igmp snooping and enter the SVGL mode.
ip igmp snooping ivgl-svgl	Enable igmp snooping and enter the hybrid mode

8.1.27 ip igmp snooping tunnel

Configure the relationship between IGMP Snooping and QinQ:

ip igmp snooping tunnel

no ip igmp snooping tunnel

Parameter description

Parameter	Description
-	-

Default	IGMP Passthrough is disabled.
Command mode	Global configuration mode.
Usage guidelines	After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways through IGMP Snooping: ■ 1st way: Create multicast entries in the VLAN to which the IMGP packets belong, and forward IMGP packets in such VLAN. For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10. ■ 2nd way: Create multicast entries in the default VLAN to which the dot1q-tunnel ports belong, and forward multicast packets in the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port. For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1. By default, the 2nd way is used.
Examples	The following example enables the IGMP packets

transparent transmission on the device:

```
DES-7200(config)# ip igmp snooping tunnel
```

Related commands

Command	Description
-	-

8.1.28 ip igmp snooping vlan

Use this command to enable the igmp snooping on the specified vlan and enter the ivgl mode. The **no** form of this command is used to disable the igmp snooping.

ip igmp snooping vlan *vid*

no ip igmp snooping vlan *vid*

Parameter description

Parameter	Description
vid	VLAN ID

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

Use this command to enable or disable the IGMP snooping on the specified vlan.

The pim snooping on the specified vlan works only when the igmp snooping configured. when disabling the igmp snooping on the vlan with the pim snooping configured, it prompts to disable the pim snooping first and this execution fails.

Examples

The following example enables the igmp snooping on the vlan2.

```
DES-7200(config)# ip igmp snooping vlan 2
```

Related commands

Command	Description
ip igmp snooping ivgl	Enable the igmp and enter the ivgl mode
ip igmp snooping	Enable the igmp snooping and

	ivgl-svgl	enter the ivgl-svgl mode

8.1.29 ip igmp snooping vlan mrouter interface

Routing interface is a port through which a multicast device is directly connected to a multicast neighbouring device. To configure a multicast routing interface, execute the **ip igmp snooping vlan mrouter interface** command in the global configuration mode. The **no** form of this command is used to delete a routing interface.

ip igmp snooping vlan *vid* **mrouter interface** *interface-id*

no ip igmp snooping vlan *vid* **mrouter interface** *interface-id*

Parameter description

Parameter	Description
vid	VLAN ID of a routing interface
interface-id	Interface ID

Default N/A.

Command mode Global configuration mode.

Usage guidelines When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.

Examples The following example demonstrates how to configure a multicast routing interface on the equipment:

```
DES-7200(config)# ip igmp snooping vlan 1 mrout
erinterface fastEthernet 0/1
```

Related commands

Command	Description
ip igmp snooping source-check port	Enable the multicast source port check function.

8.1.30 ip igmp snooping vlan mrouter learn pim-dvmrp

To configure a device to listen to the IGMP query/dvmrp or PIM packets dynamically in order to automatically identify a routing interface, execute the **ip igmp snooping vlan mrouter learn** command in the global configuration mode. The **no** form of this command is used to disable the dynamic learning.

ip igmp snooping vlan *vid* **mrouter learn pim-dvmrp**

no ip igmp snooping vlan *vid* **mrouter learn pim-dvmrp**

Parameter description

Parameter	Description
vid	VLAN ID of a routing interface

Default Disabled.

Command mode Global configuration mode.

Usage guidelines With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.

Examples The following example demonstrates how to enable the dynamic routing interface learning function on the equipment:

```
DES-7200(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

Related commands

Command	Description
ip igmp snooping mrouter learn pim-dvmrp	Enable the dynamic routing interface learning function on the multicast routing port globally

8.1.31 ip igmp snooping vlan querier

To enable the IGMP querier function in VLAN, execute "**ip igmp snooping vlan querier**" global configuration command. Use **no** form of this command to disable the IGMP querier function in the corresponding VLAN.

ip igmp snooping vlan *vid* **querier**

no ip igmp snooping vlan *vid* **querier**

Parameter description

Parameter	Description
vid	VLAN ID

Default Querier function is disabled.

Command mode	Global configuration mode.
Usage guidelines	After globally enabling the IGMP querier, you must enable IGMP querier function in VLAN to effect this command. If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.
Examples	The following example enables the IGMP querier for the VLAN on the device: `DES-7200(config)# ip igmp snooping vlan 2 querier`

Related commands

Command	Description
ip igmp snooping querier	Globally enable the querier

8.1.32 ip igmp snooping vlan querier address

To enable the IGMP querier, you also need to specify a source IP address for query packets in the corresponding VLAN. Execute the global configuration command of "**ip igmp snooping vlan querier address**". Use **no** form of this command to remove the source IP address configured.

ip igmp snooping vlan *vid* **querier address** *a.b.c.d*

no ip igmp snooping vlan *vid* **querier address**

Parameter description

Parameter	Description
vid	VLAN ID
a.b.c.d	Source IP address of queries

Default	No source IP address is specified
Command mode	Global configuration mode.

Usage guidelines	After enabling the IGMP querier, you also need to configure a source IP address for query packets, so that the device can send packets normally. If no source IP address is specified in the VLAN needing to send packets, the device will verify whether the source IP address is specified globally. The device can only send query packets after finding the source IP configured, or else the querier function won't take effect. If IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.
Examples	The following example specifies the source IP of query packets in the specific VLAN on the device: `DES-7200(config)#` **`ip igmp snooping vlan`** *`3`* **`querier address 1.1.1.1`**

Related commands

Command	Description
ip igmp snooping querier address	Globally enable the source IP check

8.1.33 ip igmp snooping vlan querier max-response-time

To configure the maximum response time advertised in query packets of a specific VLAN, execute the global configuration command of "**ip igmp snooping vlan querier max-response-time**". Use **no** form of this command to restore to the default value.

ip igmp snooping vlan *vid* **querier max-response-time** *num*

no ip igmp snooping vlan *vid* **querier max-response-time**

Parameter description

Parameter	Description
vid	VLAN ID
num	Maximum response time (1-25); unit: second; default: 10

Default	Default value

Command mode	Global configuration mode.
Usage guidelines	Configure this command to specify the maximum response time to query packets of the specific VLAN. By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.
Examples	The following example specifies the maximum response time advertised in query packets of a specific VLAN: `DES-7200(config)# ip igmp snooping vlan 3 querier max-response-time 15`

Related commands

Command	Description
ip igmp snooping querier max-response-time	Globally configure the maximum response time to query packets.

8.1.34 ip igmp snooping vlan querier query-interval

To specify the interval for IGMP querier to send query packets of a specific VLAN, execute the global configuration command of "**ip igmp snooping vlan querier query-interval**". Use **no** form of this command to restore the query interval to the default value.

ip igmp snooping vlan *vid* **querier query-interval** *num*

no ip igmp snooping *vid* **querier query-interval**

Parameter description

Parameter	Description
vid	VLAN ID
num	Query interval (1-18000); unit: second; default: 60 seconds

Default	Default value

Command mode	Global configuration mode.
Usage guidelines	After globally enabling IGMP querier, the timer will be enabled for sending query packets periodically. The aging time of the timer is the query interval. Configure this command to change the query interval. If query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.
Examples	The following example configures the query interval for specific VLAN on the device: `DES-7200(config)# ip igmp snooping vlan 3 querier query-interval 100`

Related commands

Command	Description
ip igmp snooping querier query-interval	Globally configure the query interval

8.1.35 ip igmp snooping vlan querier timer expiry

To specify the expiration timer for non-querier, execute the global configuration command of "**ip igmp snooping vlan querier timer expiry**". Use **no** form of this command to restore to the default value.

ip igmp snooping vlan *vid* **querier timer expiry** *num*

no ip igmp snooping vlan *vid* **querier timer expiry**

Parameter description

Parameter	Description
vid	VLAN ID
num	Non-querier expiration timer (60-300); unit: second; default: 125 seconds

Default	Default value

Command mode	Global configuration mode.
Usage guidelines	After globally enabling the IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier. If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.
Examples	The following example configures the non-querier expiration timer for a specific VLAN: `DES-7200(config)# ip igmp snooping vlan 3 querier timer expiry 60`

Related commands

Command	Description
ip igmp snooping querier timer expiry	Globally configure the non-querier expiration timer

8.1.36 ip igmp snooping vlan querier version

Currently, the IGMP Snooping querier supports IGMPv1 and IGMPv2. To specify the version for a specific VLAN, execute the global configuration command of "**ip igmp snooping vlan querier version**". Use **no** form of this command to restore to the default setting.

ip igmp snooping vlan *vid* **querier version** *num*

no ip igmp snooping vlan *vid* **querier**

Parameter description

Parameter	Description
vid	VLAN ID
num	IGMP version number (1-2). Default value: 2.

Default	IGMPv2

Command mode	Global configuration mode.
Usage guidelines	If the IGMP querier version number has been configured in the corresponding VLAN, the value specified in VLAN will be used first.
Examples	The following example configures the IGMP querier version on the device: `DES-7200(config)# ip igmp snooping vlan 3 querier version 1`

Related commands

Command	Description
-	-

8.1.37 ip igmp snooping vlan static interface

Once IGMP snooping is enabled, a port can receive a certain multicast frame without being afftected by various IGMP messges by executing the **ip igmp snooping vlan static interface** command in the global configuration mode. The **no** form of this command is used to delete a static configuration.

ip igmp snooping vlan *vid* **static** ip-addr **interface** *interface-id*

no ip igmp snooping vlan *vid* **static** *ip-addr* **interface** *interface-id*

Parameter description

Parameter	Description
vid	VLAN ID of a routing interface
ip-addr	Multicast IP address
interface-id	Interface ID

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	Multiple multicast IP addresses can be configured for an interface.

Examples

The following example demonstrates how to configure a static multicast address on a port:

```
DES-7200(config)# ip igmp snooping vlan 1 static 224.0.0.2
interface fastEthernet 0/1
```

Related commands

Command	Description
ip igmp snooping vlan mdevice interface	Configure a multicast routing interface

8.1.38 permit

To permit the forwarding of the multicast streams in the range specified by the profile, execute the **permit** command in the profile configuration mode. In this way, the interface associated with this profile will forward the specified multicast stream only.

permit

Parameter description

N/A

Default

The forwarding of the multicast streams in the range specified by the profile is denied.

Command mode

Profile configuration mode.

Usage guidelines

First, configure the multicast range using the **range** command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration to take effective.

Examples

The following is an example of allowing the forwarding of the multicast stream 224.2.2.2:

```
DES-7200(config)# ip igmp profile 1
DES-7200(config-profile)# range 224.2.2.2
DES-7200(config-profile)# permit
```

Related commands

Command	Description
ip igmp profile	Create a profile.
range	Configure the multicast address range.

8.1.39 range

To specify the range of multicast streams, execute the **range** command in the profile configuration mode. You can specify either a single multicast address or a range of multicast addresses. Use the **no** form of the command to remove the specified multicast IP address.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter description

Parameter	Description
low-ip-address	Start address of a range
high-ip-address	End address of a range

Default N/A.

Command mode Profile configuration mode.

Usage guidelines You can specify a behavior after configuring the address range, for example deny by default. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Examples The following is an example of creating a profile whose multicast stream is in the range 224.2.2.2 to 224.2.2.244:

```
DES-7200(config)# ip igmp profile 1
DES-7200(config-profile)# range 224.2.2.2 224.2.2.244
```

Related commands

Command	Description
ip igmp profile	Create a profile.
deny	Deny the forwarding of the multicast streams in the range specified by the profile.
permit	Permit the forwarding of the multicast streams in the range specified by the profile.

8.2 showing and Monitoring Commands

8.2.1 clear ip igmp snooping gda-table

Use this command to clear the forwarding information dynamically learned.

clear ip igmp snooping gda-table

Parameter description	N/A
Command mode	Privileged EXEC mode.
Usage guidelines	-

8.2.2 debug igmp-snp

Use the following commands to turn on igmp service debug switch. The **no** form of this command closes debug switch.

debug igmp-snp

debug igmp-snp event

debug igmp-snp packet

debug igmp-snp msf

debug igmp-snp warning

undebug igmp-snp

undebug igmp-snp event

undebug igmp-snp packet

undebug igmp-snp msf

undebug igmp-snp warning

Parameter description

Parameter	Description
none	Show all debug information of IGMP Snooping.
event	Show the debug information of IGMP Snooping event.

	packet	Show the debug information of IGMP Snooping packet.
	msf	Show the debug information exchanged between the IGMP Snooping and multicast.
	warning	Show all debug information of IGMP Snooping warning.

Command mode	Privileged EXEC mode.

8.2.3 show ip igmp profile [profile-number]

Use this command to show the profile information.

show ip igmp profile

show ip igmp profile *profile-number*

Parameter description	**Parameter**	**Description**
	none	Show configuration information of all profiles.
	profile-number	Show configuration information of the designated profile.

Command mode	Privileged EXEC mode.

Examples

```
DES-7200(config-if)# show ip igmp profile
Profile    1
Permit
range 224.0.1.0,   239.255.255.255
```

8.2.4 show ip igmp snooping

Use this command to show related information of igmp snooping.

show ip igmp snooping [**gda-table** | **interfaces** | **mdevice**| **statistics** [**vlan** *vlan-id*]]

Parameter description

Parameter	Description
none	Show the function configuration of IGMP snooping.
gda-table	Show multicast forwarding rule table.
interfaces	Show the configuration of igmp snooping filtring
mdevice	Show interface configuration of multicast device.
statistics [**vlan** *vlan-id*]	Show the igmp snooping statistics.

Command mode

Privileged EXEC mode.

Examples

The following example demonstrates how to process 100 multicast group on the interface fa0/1:

```
DES-7200(config-if)# ip igmp snooping gda-table
Abbr:M - mrouter
D – dynamic
S – static
VLAN    Address          Member ports
----------------------------------------
1      233.3.3.3         Gi0/2(S)
2      234.4.4.4         Gi0/11(S)
1      233.4.4.4         Ag2(S)
```

9 MLD Snooping Commands

9.1 Configuration Related Commands

9.1.1 ipv6 mld profile

The MLD profile is used to set a series of the group filter. Before entering the profile mode, a profile must be configured in the global configuration mode. This is a mode navigation command. You can choose the profile-number and enter the mld profile configuration mode.

ipv6 mld profile *profile-number*

no ipv6 mld profile *profile-number*

Parameter description

Parameter	Description
profile-number	Set the profile numner. The valid range is 1-1024.

Default Settings

N/A

Command mode

Global configuration mode.

Usage guidelines

MLD Profile is the group filter for the usage of the “multicast address range in the SVGL mode”, “multicast data filtering range of the route interface”, “MLD Filtering range”. To this end, to make the profile effective, the profile and the specific function shall be associated.

Examples

The following example shows how the profile 1 enter the profile configuration mode:

```
DES-7200(config)# ipv6 mld profile 1
DES-7200(config-profile)#
```

Related commands

Command	Description
range	Set the profile multicast address range.
deny	Set the profile action deny.
permit	Set the profile action permit.

9.1.2 range

Use this command to specify the profile multicast flow range, which can be one single multicast address, or can be the multicast address within the specified range when configuring a profile in the profile configuration mode. Use the no form of this command to remove the specified multicast address.

range *low-ipv6-address* [*high-ipv6-address*]

no range low-ipv6-address [high-ipv6-address]

Parameter description

Parameter	Description
low-ipv6-address	The low address within the specified range.
high-ipv6-address	The high address within the specified range.

Default Settings

N/A

Command mode

Profile configuration mode.

Usage guidelines

The value of low-ipv6-address shall be smaller than the one of high-ipv6-address. With the address range configured, an action shall be specified, and the default profile action is deny.

Examples

The following example shows how to create the multicast flow profile within the range of FF77::1~FF77::100:

```
DES-7200(config)# ipv6 mld profile 1
DES-7200(config-profile)# range FF77::1 FF77::100
```

Related

Command	Description

ipv6 mld profile	Create one profile.
deny	Set the profile action deny.
permit	Set the profile action permit.

9.1.3 deny

Use this command to prevent the multicast flow profile within the specified range from being forwarded in the profile configuration mode.

deny

Parameter description

Parameter	Description
-	-

Default Settings

The default profile action is deny.

Command mode

Profile configuration mode.

Usage guidelines

Before configuring this command, use the **range** command to set the multicast range first.

Examples

The following example shows how to prevent the multicast flow profile within the range of FF77::100 from being forwarded:

```
DES-7200(config)# ipv6 mld profile 1
DES-7200(config-profile)# range FF77::100
DES-7200(config-profile)# deny
```

Related commands

Command	Description
ipv6 mld profile	Create one profile.
range	Set the multicast address range.
permit	Set the profile action permit.

9.1.4 permit

Use this command to allow the multicast flow profile within the specified range in the profile configuration mode.

permit

Parameter description

Parameter	Description
-	-

Default Settings

The default profile action is deny.

Command mode

Profile configuration mode.

Usage guidelines

Before configuring this command, use the **range** command to set the multicast range first.

Examples

The following example shows how to allow the multicast flow profile within the range of FF77::1 to be forwarded only:

```
DES-7200(config)# ipv6 mld profile 1
DES-7200(config-profile)# range FF77::1
DES-7200(config-profile)# permit
```

Related commands

Command	Description
ipv6 mld profile	Create one profile.
range	Set the multicast address range.
deny	Set the profile action deny.

9.1.5 ipv6 mld snooping ivgl

Use this command to enable the mld snooping and specify the ivgl mode in the global configuration mode. Use the **no** form of this command to disable this function.

ipv6 mld snooping ivgl

no ipv6 mld snooping

Parameter description

Parameter	Description
-	-

Default Settings

Diabled.

Command mode	Global configuration mode.
Usage guidelines	In this mode, the multicast flow between the VLANs are independent. The host can only request for receiving the multicast flow from the route port in the same VLAN. When receiving the multicast flow from any VLAN, the switch forwards them to the member port in the same VLAN.
Examples	The following example shows how to enable the mld snooping and set the ivgl mode: `DES-7200(config)# ipv6 mld snooping ivgl`

Related commands

Command	Description
ipv6 mld snooping svgl	Enable the mld snooping and set the svgl mode.
ipv6 mld snooping ivgl-svgl	Enable the mld snooping and set the ivgl-svgl mode.

9.1.6 ipv6 mld snooping svgl

Use this command to enable the mld snooping and specify the svgl mode in the global configuration mode. Use the **no** form of this command to disable this function.

ipv6 mld snooping svgl

no ipv6 mld snooping

Parameter description

Parameter	Description
-	-

Default Settings	Diabled.
Command mode	Global configuration mode.
Usage	In the SVGL mode, the hosts in each VLAN share the

guidelines	multicast flow and can apply for the multicast flow across VLANs. Only the multicast flow in the specified Shared VLAN can be forwarded to other hosts across the VLANs. If the multicast flow belong to the Shared VLAN, they can be forwarded to the member port of this multicast address, even if some member ports don't belong to the Shared VLAN. In the SVGL mode, use the MLD profile to allocate a batch of multicast address range, within which the member port of the multicast forwarding entry can be forwarded across the VLANs. By default, the range of all groups is beyond the SVGL range and all multicast flow are discarded. To this end, a profile used to specifued the multicast address range in the SVGL mode must be associated for the normal runnning of the SVGL mode.
Examples	The following example shows how to enable the mld snooping and set the svgl mode(the specified profile1 group address belongs to the SVGL application range): `DES-7200(config)# ipv6 mld snooping svgl profile 1`

Related commands

Command	Description
ipv6 mld snooping ivgl	Enable the mld snooping and set the ivgl mode.
ipv6 mld snooping ivgl-svgl	Enable the mld snooping and set the ivgl-svgl mode.

9.1.7 ipv6 mld snooping svgl profile

Use this command to specify the group address range to be in the SVGL mode. Use the **no** form of this command to cancel this association.

ipv6 mld snooping svgl profile *profile-number*

no ipv6 mld snooping svgl profile

Parameter description

Parameter	Description
profile-number	Set the profile number. The valid range is 1-1024.

Default Settings	Diabled.

Command mode	Global configuration mode.
Usage guidelines	With the SVGL mode or IVGL-SVGL mode configured for the MLD Snooping working mode, a profile shall be associated with the IVGL for the purpose of specifying the group address range in the SVGL mode. That is to say, the member port of the multicast forwarding entry can be forwarded across the VLANs, while the member ports of the corresponding multicast forwarding entries within other multicast address range must belong to the same VLAN. By default, no profile is associated, which means that apply no multicast group in the SVGL mode.
Examples	The following example shows how to specify the SVGL mode application range as the profie1 group address range: `DES-7200(config)# ipv6 mld snooping svgl profile 1`

Related commands

Command	Description
ipv6 mld snooping ivgl	Enable the mld snooping and set the ivgl mode.
ipv6 mld snooping ivgl-svgl	Enable the mld snooping and set the ivgl-svgl mode.

9.1.8 ipv6 mld snooping ivgl-svgl

Use this command to enable the mld snooping and specify the ivgl-svgl mode in the global configuration mode. Use the **no** form of this command to disable this function.

ipv6 mld snooping ivgl-svgl *profile-number*

no ipv6 mld snooping ivgl-svgl

Parameter description

Parameter	Description
profile-number	Set the profile number. The valid range is 1-1024.

Default Settings	Diabled.

Command mode	Global configuration mode.
Usage guidelines	IVGL-SVGL mode: the IVGL mode and the SVGL mode co-exist. Use the MLD Profile to allocate a batch of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across the VLANs, while the member ports of the corresponding multicast forwarding entries within other multicast address range must belong to the same VLAN.

Examples	The following example shows how to enable the mld snooping and set the ivgl-svgl mode(the specified profile1 group address belongs to the SVGL application range):
	`DES-7200(config)# ipv6 mld snooping ivgl-svgl`
	`DES-7200(config)# ipv6 mld snooping svgl profile 1`

Related commands

Command	Description
ipv6 mld snooping ivgl	Enable the mld snooping and set the ivgl mode.
ipv6 mld snooping ivgl-svgl	Enable the mld snooping and set the ivgl-svgl mode.

9.1.9 ipv6 mld snooping dyn-mr-aging-time

Use this command to set the aging time of the dynamic multicast route port. Use the **no** form of this command to restore it to the default value.

ipv6 mld snooping dyn-mr-aging-time *time*

no ipv6 mld snooping dyn-mr-aging-time

Parameter description

Parameter	Description
time	Set the aging time of the dynamic multicast route port, in seconds. The valid range is 1-3600.

Default Settings	300s.
Command mode	Global configuration mode.

Usage guidelines	The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the Ipv6 PIM Hello packets within the aging timeout on this interface.
Examples	The following example shows how to set the aging time of the dynamic multicast route port as 500s: `DES-7200(config)# ipv6 mld snooping dyn-mr-aging-time 500`

9.1.10 ipv6 mld snooping query-max-response-time

Use this command to set t the maximum response time of the MLD general query packet. Use the **no** form of this command to restore it to the default value.

ipv6 mld snooping query-max-response-time *time*

no ipv6 mld snooping query-max-response-time

Parameter description

Parameter	Description
time	Set the maximum response time of the MLD general query packet, in seconds. The valid range is 1-65535.

Default Settings	10s.
Command mode	Global configuration mode.
Usage guidelines	Upon receiving the MLD general query packets, the Layer-2 multicast device updates the aging timer of all member ports. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list. Upon receiving the MLD specific group query packets, the Layer-2 multicast device enables the aging timer of all member ports in this specific group. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD

	Snooping forwarding list. For the source query packets of the MLD specific group, the timer is not updated.
Examples	The following example shows how to set the maximum response time of the MLD general query packet as 15s: `DES-7200(config)# ipv6 mld snooping query-max-response-time 15`

9.1.11 ipv6 mld snooping vlan

Use this command to enable the mld snooping function for the specified vlan. Use the **no** form of this command to disable this function.

ipv6 mld snooping vlan *vid*

no ipv6 mld snooping vlan *vid*

Parameter description

Parameter	Description
vid	The vlan id number. The valid range is 1-4094

Default Settings	By default, the mld snooping is enabled in all VLANs.
Command mode	Global configuration mode.
Usage guidelines	By default, the mld snooping is enabled in all VLANs. You can disable the mld snooping for the specified vlan.
Examples	The following example shows how to disable the mld snooping function in vlan1: `DES-7200(config)# no ipv6 mld snooping vlan 1`

9.1.12 ipv6 mld snooping vlan mrouter learn

Use this command to enable the switch to dynamically learn MLD query or PIM packets to identify the mrouter interface automatically. Use the **no** form of this command to restore it to cancel the dynamic learning.

ipv6 mld snooping vlan *vid* **mrouter learn**

no ipv6 mld snooping vlan *vid* **mrouter learn**

Parameter description

Parameter	Description
vid	The vlan id, with the valid range 1-4094.

Default Settings

Diabled.

Command mode

Global configuration mode.

Usage guidelines

The mrouter interface is the interface of the multicast device connected with the peer device. By default, the dynamically-learned mroute interface is enabled on the layer-2 multicast device. Use the **no** option to disable this function and clear all dynamically-learned mroute interfaces. With the source port check enabled, only the multicast flow through the mroute interface are valid and forwarded to the registered interface on the layer-2 multicast device. Those multicast flow through the non-mroute interface are invalid and will be discarded. With the source port check function enabled, use the dynamically-learned mroute interfaces to improve the mld snooping flexibility.

Examples

The following example shows how to enable the dynamic multicast route port learn function:

```
DES-7200(config)# ipv6 mld snooping vlan 1 mrouter learn
```

Related commands

Command	Description
ipv6 mld snooping vlan mrouter interface	Set the mrouter interface.

9.1.13 ipv6 mld snooping vlan mrouter interface

Use this command to set the static mrouter interface. Use the **no** form of this command to delete a static mrouter interface.

ipv6 mld snooping vlan *vid* **mrouter interface** *interface-id*

no ipv6 mld snooping vlan *vid* **mrouter interface** *interface-id*

Parameter description

Parameter	Description
vid	The vlan id, with the valid range 1-4094.
Interface-id	The interface number.

Default Settings

N/A.

Command mode

Global configuration mode.

Usage guidelines

Use this command to set the static mrouter interface for the purpose that all IPv6 multicast data received on the switch can be forwarded. With the source port check function enabled, only the multicast flow through the mroute interface can be forwarded.

Examples

The following example shows how to set a multicast routing port:

```
DES-7200(config)# ipv6 mld snooping vlan 1 mrouter interface fastEthernet 0/1
```

Related commands

Command	Description
ipv6 mld snooping source-check port	Set the multicast source port check.

9.1.14 ipv6 mld snooping vlan static interface

Use this command to set a static member port to receive the multicast flow for the purpose of preventing the port from being inflenced by the MLD Report packets with the MLD Snooping enabled. Use the **no** form of this command to delete a static member port.

ipv6 mld snooping vlan *vid* **static** *ipv6-multiaddr* **interface** *interface-id*

no ipv6 mld snooping vlan *vid* **static** *ipv6-multiaddr* **interface** *interface-id*

Parameter description

Parameter	Description
vid	The vlan id, with the valid range 1-4094.
ipv6-multiaddr	The multicast address.

	interface-id	The interface number.

Default Settings N/A.

Command mode Global configuration mode.

Usage guidelines Use this command to set the interface as the member port of multiple static multicast addresses.

Examples The following example shows how to set the interface fastEthernet 0/1 as the static member port of the FF88::1 group:

```
DES-7200(config)# ipv6 mld snooping vlan 1 static FF88::1 interface fastEthernet 0/1
```

Related commands

Command	Description
ipv6 mld snooping vlan mrouter interface	Set the mrouter interface.

9.1.15 ipv6 mld snooping fast-leave enable

Use this command to enable the mld snooping fast-leave in the global configuration mode. Use the **no** form of this command to disable this function.

ipv6 mld snooping fast-leave enable

no ipv6 mld snooping fast-leave enable

Parameter description

Parameter	Description
-	-

Default Settings N/A

Command mode Global configuration mode.

Usage The interface fast leave is that when IPv6 MLD Leave

guidelines	packets sent from the host are received on an interface, the interface is removed form the outgoing interface list of the corresponding forwarding entry. Then, the switch will not forward the received IPv6 MLD specific group query packets to the interface. If there is only one receiver connected with the interface, enable the interface fast leave function to save the bandwidth and resources.
Examples	The following example shows how to enable mld snooping fast-leave: `DES-7200(config-if)# ipv6 mld snooping fast-leave`

9.1.16 ipv6 mld snooping suppression enable

Use this command to enable the mld snooping suppression in the global configuration mode. Use the **no** form of this command to disable this function.

ipv6 mld snooping suppression enable

no ipv6 mld snooping suppression enable

Parameter description

Parameter	Description
-	-

Default Settings	N/A
Command mode	Global configuration mode.
Usage guidelines	With the IPv6 MLD snooping suppression function enabled, within the query interval, the layer-2 device will only forward the first received MLD Report packet in an IPv6 multicast group to the layer-3 device, but not the other MLD Report packets in the same IPv6 multicast group, reducing the packet number in the network. This command is used to enable the IPv6 MLD snooping suppression, and only the MLDv1 Report packets are suppressed rather than the MLDv2 Report packets.
Examples	The following example shows how to enable mld snooping suppression:

```
DES-7200(config-if)# ipv6 mld snooping suppression
```

9.1.17 ipv6 mld source-check port

The source-check port is used to allow the multicast flow to enter through the mrouter interface. Use this command to enable the mld source-check port in the global configuration mode. Use the **no** form of this command to disable this function.

ipv6 mld snooping source-check port

no ipv6 mld snooping source-check port

Parameter description

Parameter	Description
-	-

Default Settings

N/A

Command mode

Global configuration mode.

Usage guidelines

The MLD Snooping source port check function is to limit the MLD multicast flow through the interace strictly. With the source port check disabled, all video flow are illegal and forwarded to the registered member port according to the MLD Snooping forwarding list. With the MLD Snooping source port check enabled, only the mulitcast flow through the mroute interface is legal and forwarded to the registered interface by the layer-2 multicast device; and the multicast flow through the non-mroute interface are illegal and discarded.

This command is used to enabled the source port check globally. Once this function is enabld, all multicast flow must come from the mroute interface, or they'll be discarded.

Examples

The following example shows how to enable mld snooping source-check port:

```
DES-7200(config-if)# ipv6 mld snooping source-check port
```

9.1.18 ipv6 mld snooping filter

Use this command to filter the specific multicast flow in the interface configuration mode. Use the **no** form of this command to delete the associated profile.

ipv6 mld snooping filter *profile-number*

no ipv6 mld snooping filter *profile-number*

Parameter description

Parameter	Description
profile-number	Set the profile number.

Default Settings

N/A.

Command mode

Interface configuration mode.

Usage guidelines

You can configure an MLD Profile on an interface. If the MLD Report packets are received on the interface, the layer-2 device will determine whether the multicast address to be joined the interface is within the allowed range of the MLD Profile. The specified profile must be created before using this command.

Examples

The following example shows how to associate profile1 with the interface fastEthernet 0/1:

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ipv6 mld snooping filter 1
```

Related commands

Command	Description
ipv6 mld profile	Create a profile.

9.1.19 ipv6 mld snooping max-groups

Use this command to set the maximum group allowed to join the interface dynamically in the interface configuration mode. Use the no form of this command to cancel the limit.

ipv6 mld snooping max-groups *number*

no ipv6 mld snooping max-groups

Parameter description

Parameter	Description
number	The valid range is 0-1024.

Default Settings

1024

Command mode

Interface configuration mode.

Usage guidelines

With this command configured, when the group number exceeds the specified range on the interface, the switch will not receive and deal with the MLD Report packets.

Examples

The following example shows how to set the maximum 100 multicast group on the interface fastEthernet 0/1:

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ipv6 mld snooping max-group 100
```

Related commands

Command	Description
ipv6 mld snooping filter	Fliter the multicast group on the interface.

9.1.20 clear ipv6 mld snooping gda-table

Use this command to clear the forwarding table information learned dynamically.

clear ipv6 mld snooping gda-table

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage

Use this command to clear the forwarding table

guidelines	information learned dynamically.
Examples	The following example shows how to clear the forwarding table information learned dynamically: `DES-7200# clear ipv6 mld snooping gda-table`

9.1.21 debug mld-snp

Use this command to enable the mld service debugging switch.

debug mld-snp

undebug mld-snp

Parameter description

Parameter	Description
-	-

Default Settings	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to enable the mld service debugging switch.
Examples	The following example shows how to enable the mld service debugging switch: `DES-7200# debug mld-snp`

9.2 Showing Related Commands

9.2.1 show ipv6 mld snooping

Use this command to show the related mld snooping information.

show ipv6 mld snooping [gda-table | interfaces | mrouter| statistics | vlan *vlan-id*]

Parameter description

Parameter	Description
-	Show the mld snooping configurations.
gda-table	Show the multicast

	forwarding rule table.
interfaces	Show the mld snooping filtering configuration.
mrouter	Show the information about mrouter interface.
statistics	Show the snooping statistics.
vlan *vlan-id*	Show the snooping information of the specified vlan.

Default Settings N/A.

Command mode Privileged EXEC mode.

Usage guidelines Use this command to show the related mld snooping information.

Examples

The following example shows the mld snooping configurations using the **show ipv6 mld snooping** command:

```
DES-7200# show ipv6 mld snooping
MLD-snooping mode      : IVGL
SVGL vlan-id           : 1
SVGL profile number    : 0
Source check port      : Disabled
Query max respone time : 10(Seconds)
```

The following example shows the mrouter interface of the mld snooping using the **show ipv6 mld snooping statistics** command:

```
DES-7200# show ipv6 mld snooping statistics
GROUP   Interface  Last report    Last leave     Last
                       time       time         reporter
------------------------- ------------ -------------
FF88::1 VL1:Gi4/2    0d:0h:0m:7s     ----     2003::1111
                     Report pkts: 1       Leave pkts: 0
```

The following example shows the mrouter interface of the mld

snooping using the **show ipv6 mld snooping mrouter** command:

```
DES-7200# show ipv6 mld snooping mrouter
Vlan    Interface       State     MLD profile number
----     --------         -------     -------------------
1   GigabitEthernet 0/7    static        1
1   GigabitEthernet 0/12   dynamic       0
```

The following example shows the multicast group information in the GDA table and all member ports information of one multicast group:

```
DES-7200# show ipv6 mld snooping gda-table
Abbr: M - mrouter
     D - dynamic
     S - static
VLAN  Address            Member ports
-----------------------------------------------------------
1      FF88::1          GigabitEthernet 0/7(S)
```

The following example shows the mld snooping filtering configuration using the **show ipv6 mld snooping mrouter** command:

```
DES-7200# show ipv6 mld snooping interface GigabitEthernet
0/7
Interface         Filter Profile number     max-groups
----------       ----------------------    -----------
GigabitEthernet 0/7          1              4294967294
```

9.2.2 show ipv6 mld profile

Use this command to show the related MLD profile configurations.

show ipv6 mld profile [*profile-number*]

Parameter description

Parameter	Description
-	Show the configurations of all profiles.
profile-number	Show the configuration of the specified profile.

Default Settings	N/A
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to show the related MLD profile configurations.

Examples	The following example shows the MLD profile configurations:
	`DES-7200# **show ipv6 mld profile** *1*`
	`MLD Profile 1`
	`permit`
	`range FF77::1 FF77::100`
	`range FF88::123`

10 PIM Snooping Commands

10.1 Configuration Related Command

10.1.1 ip pim snooping (global configuration mode)

This command enables or disables the PIM snooping globally.

ip pim snooping

no ip pim snooping

Parameter description	N/A
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The normal PIM-Snooping function must depend on the IVGL or IVGL-SVGL mode of IGMP-Snooping. The IVGL mode of IGMP-Snooping are enabled when configuring the PIM-Snooping if the IGMP-Snooping is not enabled globally. The PIM-Snooping configuration will fail if the SVGL mode of IGMP-Snooping is enabled globally. Thus, the SVGL mode of IGMP-Snooping must be disabled first to enable the PIM-Snooping. If you disable PIM Snooping globally, then the PIM Snooping function will be ineffective in all VLANs.
Examples	`DES-7200# configure terminal` `DES-7200(config)# ip pim snooping`

10.1.2 ip pim snooping (interface configuration mode)

This command enables or disables the PIM snooping on the interface.

ip pim snooping

no ip pim snooping

Parameter description	N/A
Default	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	The normal PIM-Snooping function must depend on the IGMP-Snooping. If the IGM-Snooping in the VLAN is not enabled, the user will be informed of enabling the IGMP-Snooping for the VLAN first and the failed configuration when configuring the PIM-Snooping. If you disable PIM Snooping globally, then the PIM Snooping function will be ineffective in all VLANs.

Examples	`DES-7200# configure terminal`
	`DES-7200(config)# interface vlan 199`
	`DES-7200(config-if)# ip pim snooping`

10.1.3 show ip pim snooping

Use this command to show global configuration information of PIM snooping.

show ip pim snooping [**detail**]

Parameter description

Parameter	Description
detail	Show the detailed information.

Command mode	Privileged EXEC mode / User mode.

Examples	The following example shows the global configuration information of the PIM snooping function:
	`DES-7200#`**`show ip pim snooping`**
	`Global runtime mode : Enabled`
	`Global admin mode : Enabled`
	`Number of user enabled VLANs: 2`
	`User enabled VLANs: 199 198`

10.1.4 show ip pim snooping neighbor

Use this command to display the PIM Snooping neighbor information.

show ip pim snooping neighbor

Parameter description	N/A
Command mode	Privileged EXEC mode / User mode

Examples	The following example shows the information of the PIM snooping neighbor:
	`DES-7200#`**`show ip pim snooping neighbor`**
	`IP Address Port Uptime/Expires Flags`
	`VLAN 199: 2 neighbors`
	`214.199.199.2 2/32 00:18:25/00:01:04`
	`214.199.199.10 2/20 00:18:09/00:01:03 DR`

10.1.5 show ip pim snooping vlan

Use this command to display related information of PIM-Snooping VLAN.

show ip pim snooping vlan *interface-number* [neighbor]

Parameter description

Parameter	Description
interface-number	Show VLAN ID.
neighbor	Show the neighbor information in the VLAN.

Command mode	Privileged EXEC mode / User mode

Examples	The following example shows the information of the PIM Snooping VLAN 199: DES-7200# show ip pim snooping vlan 199 4 neighbors (0 DR priority incapable) DR is 214.199.199.4

DES-7200

MPLS Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 MPLS Configuration Commands

1.1 Basic MPLS Configuration Commands

1.1.1 advertise-labels

Use this command to configure the policy for distributing a label to an IP route Forwarding Equivalence Class (FEC).

[**no**] **advertise-labels** [**for host-routes** | **for bgp-routes** [**acl** *acl_name*]| **for default-route | for acl** *prefix-access-list* [**to** *peer-access-list*]

Parameter description

Parameter	Description
for host-routes	(Optional) Distribute labels to host routes (the subnet mask is 32-bit long) only.
for bgp-routes [**acl** *acl_ame*]	(Optional) Distribute labels to BGP routes only. You can distribute labels to only the BGP routes meeting conditions by using ACL keywords.
for default-route	(Optional) Distribute non-3 labels to default routes.
for acl *prefix-access-list*	(Optional) Specify the prefix of the routes to which labels are distributed.
to *peer-access-list*	(Optional) Specify the neighbors to which label binding information is sent.

Default configuration

By default, labels are distributed to all LDP neighbors.

By default, labels are distributed to all IGP routes instead of BGP routes, for which FTN is not added either.

By default, implicit null label 3 is distributed to default routes.

Command mode	**config-mpls-router** mode
Usage guidelines	This command is effective to only the IP route FEC instead of other FECs such as PW FEC. Use the **advertise-labels for acl** *fec_acl* **to** *peer_acl* command to specify the FECs and LDP peers to which labels are distributed. For specified fec_acl, only one rule can be configured; for peer-acl, multiple rules can be configured. If this command is configured but no filtering rule is configured in the corresponding ACL, it is equivalent that this command is not configured, that is, FEC label mapping messages are sent normally. A label request received by an LDP session working in DOD mode cannot be replied with a label mapping message if the request cannot meet the lable distribution policy as a result of the configured rule. Even if the rule is cancelled afterwards, the request that has been filtered cannot be distributed with a label mapping message. In this case, you can use the **clear mpls ldp neighbor** command to reset the LDP session to make it return to normal. You can use this command to confiugre a maximum of 64 rules. Use the **advertise-labels for bgp-routes** command to distribute labels to BGP routes. You can use this command with the acl option to distribute labels to BGP routes meeting conditions or use this command without the acl option to distribute labels to all BGP routes. Use the **no advertise-labels for bgp-routes** command to disable the distribution of labels to BGP routes. Note that the distribution of labels to BGP routes is still controlled by the label distribution policy of LDP. Use the **advertise-labels for host-routes** command to distribute lables only to route prifexes with 32-bit masks (namely host routes). Use the **advertise-labels for default-route** command to distribute non-3 lables to default routes, thus establishing an LSP for default routes.

Labels are distributed to all FECs by default. Therefore, you must use the no advertise-labels command to disable the distribution of labels to all FECs if you want to distribute labels to only the FECs meeting specified ACL rules. In this manner, labels are not distributed to those failing to meet ACL rules.

Caution

After the no advertise-labels command is configured, labels are distributed to only the FECs meeting advertise-labels for acl *prefix-access-list* [to *peer-access-list*] and instead of other FECs. If the preceding rule is not met, labels are not distributed to BGP routes and host routes even if the advertise-labels for bgp-routes command or advertise-labels for host-routes command is configured.

When the advertise-labels for host-routes command is configured, LDP distributes labels to only host routes and adds FTN for only host routes.

Examples

Example 1: The following command sets the LDP instance to distribute labels to the host route FEC only:

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# advertise-labels for host-routes
```

Example 2: The following command sets the LDP instance not to distribute any label to the LDP peer of the IP route FEC:

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# no advertise-labels
```

Example 3: The following command sets the LDP instance to distribute labels to all LDP peers of the FEC with 192.168.0.0/16 as the route prefix:

```
DES-7200(config)#ip access-list standard fec_acl
DES-7200(config-std-nacl)#permit 192.168.0.0 0.0.255.255
DES-7200(config-std-nacl)# exit
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# no advertise-labels
DES-7200(config-mpls-router)# advertise-labels for acl fec_acl
```

Example 4: The following command sets the LDP instance to distribute

labels to LDP peer 6.6.6.6 and LDP peer 7.7.7.7 of the FEC with 192.168.0.0/24 as the route prefix but to all LDP peers of other FECs:

```
DES-7200(config)#ip access-list standard fec_acl
DES-7200(config-std-nacl)#permit 192.168.0.0 0.0.0.255
DES-7200 (config)#ip access-list standard peer_acl
DES-7200 (config-std-nacl)#permit host 6.6.6.6
DES-7200 (config-std-nacl)#permit host 7.7.7.7
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# advertise-labels for acl fec_acl to peer_acl
```

Related commands

Command	Description
-	-

Platform description

None

1.1.2 backoff

Use this command to configure the time for LDP exponential backoff. Use the **no** form of this command to restore the default value.

backoff initial-backoff maximum-backoff

no backoff

Parameter description

Parameter	Description
initial-backoff	Indicate the initial time of exponential backoff in the unit of second, ranging from 5 to 2147483, 15 by default.
maximum-backoff	Indicate the maximum time of backoff in the unit of second, ranging from 5 to 2147483, 120 by default.

Default configuration

By default, the initial time of exponential backoff is 15s and the maximum time is 120s.

Command mode	**config-mpls-router** mode
Usage guidelines	When the LSR acts as the active side, the LDP session cannot be established if the parameters for negotiation are found inconsistent during the establishment of the LDP session. In this case, the LSR keeps attempting to re-establish an LDP session, which wastes system resources. The exponential backoff mechanism is just to prevent the active side from attempting to re-establish an LDP session constantly. The active side attempts to re-establish an LDP session only when the backoff time times out or the CSN of the Help message from the peer changes (which means changes in the configuration of the peer).

Examples	The following command can require the initial time of exponential backoff to be 20s and the maximum time to be 300s in this instance:
	`DES-7200(config)# mpls router ldp`
	`DES-7200(config-mpls-router)# advertise-labels for bgp-routes`

Related commands

Command	Description
show mpls ldp parameters	Show the configuration parameters of the LDP instance.

1.1.3 bfd bind backward-lsp-with-ip

Use this command to configure BFD to detect whether the LSP backward link uses an IP address. Use the **no** form of this command to disable this detection function.

bfd bind backward-lsp-with-ip peer-ip ***ip-address*** **[vrf** ***vrf-name*****] interface** ***interface-type interface-number*** **[source-ip** ***ip-address*****] local-discriminator** ***discr-value*** **remote-discriminator** ***discr-value***

no bfd bind backward-lsp-with-ip peer-ip *ip-address* [**vrf** *vrf-name*]

Parameter description

Parameter	Description
peer-ip *ip-address*	Peer IP address bound by the BFD session

vrf *vrf-name*	VRF name bound by the BFD session
interface *interface-type interface-number*	Configure the interface type and interface number.
source-ip *ip-address*	Source IP address carried by the BDF session
local-discriminator *discr-value*	Configure the local identifier of the current BFD session, ranging from 1 to 8191.
remote-discriminator *discr-value*	Configure the remote identifier of the current BFD session, ranging from 1 to 8191.
no	Disable the function for BFD to detect whether the LSP backward link uses an IP address.

Default configuration

By default, this function is disabled.

Command mode

Global configuration mode

Usage guidelines

Use this command to configure BFD to detect whether the LSP backward link uses an IP address as follows:

- If the LSP backward link uses an IP address, the forward LSP must be configured with a local identifier and a remote identifier, that is, manual configuration mode must be adopted.
- The peer IP address needs to be configured, and the source IP address is optional.
- In the case of having no specified source IP address, the source IP address in the BFD packet is not updated if the IP address of the outgoing interface is changed after the BFD session is configured successfully. In the case of having a specified source IP address, the source IP address in the BFD packet is not updated if the source IP address is changed after the BFD session is configured successfully. After the BFD session is established successfully, the identifier cannot be modified.
- The system regularly queries the BFD configuration items that sessions have been submitted but not been established and attempts to establish BFD sessions.
- The system has a limit on the number of BFD sessions. If the number of BFD sessions submitted and established by a user exceeds the upper limit allowed by the system, the system will generate log information to prompt the user.

Examples

In global configuration mode on the switch, the following command configures BFD to detect whether the LSP backward link uses an IP address. The source IP address is 20.20.20.20, and the destination IP address is 10.10.10.10. The outgoing interface is GigabitEthernet 0/2. The local identifier is 1, and the remote identifier is 2. The configuration is as follows:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
DES-7200(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100
multiplier 3
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#bfd bind backward-lsp-with-ip peer-ip 10.10.10.10
interface gigabitEthernet 0/2 source-ip 20.20.20.20
local-discriminator 1 remote-discriminator 2
```

Related commands	

Command	Description
bfd	Configure the parameters of the LDP session.

Platform description	None

1.1.4 bfd bind ldp-lsp

Use this command to configure BFD to detect LDP LSP. Use the **no** form of this command to disable this function.

bfd bind ldp-lsp peer-ip ***ip-address*** **nexthop** ***ip-address*** **[interface** ***interface-type interface-number*****] source-ip** ***ip-address*** **[local-discriminator** ***discr-value*** **remote-discriminator** ***discr-value*****] [process-state]**

no bfd bind ldp-lsp peer-ip *ip-address*

Parameter description

Parameter	Description
peer-ip *ip-address*	Bind the sink IP address of the LDP LSP by the BFD session.
nexthop *ip-address*	Specify the next-hop IP address of LDP LSP.
interface *interface-type interface-number*	Configure the interface type and interface number.
source-ip *ip-address*	Source IP address carried by the BFD packet
local-discriminator *discr-value*	Configure the local identifier of the current BFD session, ranging from 1 to 8191.
remote-discriminator *discr-value*	Configure the remote identifier of the current BFD session, ranging from 1 to 8191.
process-state	Process the state of the current BFD session. For some applications requiring BFD to detect faults such as delpoyments based on the cooperation BFD and LSP, this parameter is mandatory.
no	Mean disabling this function.

Default configuration	By default, this function is disabled.
Command mode	LDP configuration mode
Usage guidelines	Use this command to configure BFD to detect an LDP LSP as follows: ■ This command can only be executed on ingress nodes of an LSP. ■ When BFD configuration has existed, the BFD configuration item cannot be established. After BFD is configured, a BFD session starts being established immediately if the LDP LSP exists. If the LDP LSP does not exist, a BFD session starts being established when the LDP LSP exists. ■ When the LDP LSP is deleted, the BFD session bound to it is deleted. However, the system reserves the configuration item of this BFD session. When the LDP LSP exists, the system re-creates a BFD session. ■ The local identifier and remote identifier can be configured in a BFD session. If the local identifier is not configured, the system elects the local identifier automatically. If the LSP backward link adopts an IP address, the forward LSP must be configured with the local identifier and remote identifier manually. ■ When the address of the egress of the detected LSP is borrowed or lent, the egress must be specified. Otherwise, the egress does not need to be specified. ■ After a BFD session is established successfully, the identifier cannot be modified. ■ The system queries regularly BFD configuration items that sessions have been submitted but not been established and attempts to establish BFD sessions. ■ The system has a limitation on the number of BFD sessions. If the number of requests for establishing BFD sessions submitted by a user exceeds the limitation, the system prompts the user through log information.

Caution

Only LDP LSP detection established by host routes is supported.

One LSP can be configured with only one BFD session.

Examples

Example 1: Autonegotiate an identifier.

In LDP configuration mode on the switch, configure BFD to detect LDP LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10, and the next-hop address is 1.1.1.2. The configuration is as follows:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
DES-7200(config-if-GigabitEthernet 0/2)#label-switching
DES-7200(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier 3
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)#bfd bind ldp-lsp peer-ip 10.10.10.10 nexthop 1.1.1.2 source-ip 20.20.20.20
```

Example 2: Specify an identifier manually.

In LDP configuration mode on the switch, configure BFD to detect LDP LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10, and the next-hop address is 1.1.1.2. The local identifier is 1, and the remote identifier is 2. The BFD session status is processed. The configuration is as follows:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
```

```
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
DES-7200(config-if-GigabitEthernet 0/2)#label-switching
DES-7200(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier 3
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)#bfd bind ldp-lsp peer-ip 10.10.10.10 nexthop 1.1.1.2 source-ip 20.20.20.20 local-discriminator 1 remote-discriminator 2 process-state
```

Related commands

Command	Description
bfd	Configure the parameters for the BFD session.

Platform description

None

1.1.5 bfd bind static-lsp

Use this command to configure BFD to detect a static LSP. Use the **no** form of this command to disable this function.

bfd bind static-lsp peer-ip ***ip-address*** **source-ip** ***ip-address*** **[local-discriminator** ***discr-value*** **remote-discriminator** ***discr-value***] **[process-state]**

no bfd bind static-lsp peer-ip *ip-address*

Parameter description

Parameter	Description
peer-ip *ip-address*	Sink IP address of the static LSP bound by the BFD session
source-ip *ip-address*	Source IP address carried by the BDF packet
local-discriminator *discr-value*	Configure the local identifier of the current BFD session, ranging from 1 to 8191.
remote-discriminator *discr-value*	Configure the remote identifier of the current BFD session, ranging from 1 to 8191.

	process-state	Process the state of the current BFD session. For some applications requiring BFD to detect faults such as delpoyments based on the cooperation BFD and LSP, this parameter is mandatory.
	no	Mean disabling this function.

Default configuration	By default, this function is disabled.

Command mode	Global configuration mode

Usage guidelines

Use this command to configure BFD to detect a static LSP as follows:

- This command can only be executed on ingress nodes of an LSP.
- When the BFD configuration has existed, the BFD configuration item cannot be established. After BFD is configured, a BFD session starts being established immediately if the static LSP exists. If the static LSP does not exist, a BFD session starts being established when the static LSP exists.
- When the static LSP is deleted, the BFD session bound to it is deleted. However, the system reserves the configuration item of this BFD session. When the static LSP exists, the system re-creates a BFD session.
- The local identifier and remote identifier can be configured in a BFD session. If the local identifier is not configured, the system elects the local identifier automatically. If the LSP backward link adopts an IP address, the forward LSP must be configured with the local identifier and remote identifier manually.
- When the address of the egress of the detected LSP is borrowed or lent, the egress must be specified. Otherwise, the egress does not need to be specified.
- After a BFD session is established successfully, the identifier cannot be modified.
- The system queries regularly BFD configuration items that sessions have been submitted but not been established and attempts to establish BFD sessions.
- The system has a limitation on the number of BFD sessions. If the number of requests for establishing BFD sessions submitted by a user exceeds the limitation, the system prompts the user through log information.

Caution

Only static LSP detection established by host routes is supported.

One LSP can be configured with only one BFD session.

Examples

Example 1: Autonegotiate an identifier.

In global configuration mode on the switch, configure BFD to detect static LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10. The confiugration is as follows:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
DES-7200(config)#mpls ip
DES-7200(config)#interface GigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
DES-7200(config-if-GigabitEthernet 0/2)#label-switching
DES-7200(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier 3
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#bfd bind static-lsp peer-ip 10.10.10.10 source-ip 20.20.20.20
```

Example 2: Specify an identifier manually.

In global configuration mode on the switch, configure BFD to detect static LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10. The local identifier is 1, and the remote identifier is 2. The BFD session state is processed. The confiugration is as follows:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface GigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
DES-7200(config-if-GigabitEthernet 0/2)#label-switching
DES-7200(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier 3
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#bfd bind static-lsp peer-ip 10.10.10.10 source-ip 20.20.20.20 local-discriminator 1 remote-discriminator 2 process-state
```

Related commands

Command	Description
bfd	Configure the parameters for the BFD session.

Platform description

None

1.1.6 clear mpls ldp neighbor

Use this command to forcibly disconnect an LDP session and re-establish an LDP session.

clear mpls ldp neighbor [**all** | **vrf** *vrf-name*] {* | *ip-address*}

Parameter description

Parameter	Description
all	Forcibly disconnect LDP sessions under all virtual routing and forwarding instances (VRFs, including default global VRF) and re-establish sessions.
vrf *vrf-name*	Forcibly disconnect LDP sessions under specified VRFs and re-establish sessions.
*	Forcibly disconnect LDP sessions under specified VRFs or all VRFs and re-establish sessions.
ip-address	Forcibly disconnect LDP sessions established between specified VRFs or all VRFs and specified LDP peers and re-establish sessions.

Default configuration

None

Command mode

Privileged mode

Usage guidelines

If no VRF is specified in this command, it indicates that LDP sessions under the default global VRF are forcibly reset.

Examples

The following command forcibly resets all established LDP sessions under the default global VRF:

```
DES-7200# clear mpls ldp neighbor *
```

The following command forcibly resets the LDP sessions established between the default global VRF and the peer 10.10.10.10:

```
DES-7200# clear mpls ldp neighbor 10.10.10.10
```

The following command forcibly resets the LDP sessions established

under all VRFs (including default global VRF):

```
DES-7200# clear mpls ldp neighbor all *
```

Related commands

Command	Description
show mpls ldp neighbor	Show the state of the LDP session.

Platform description

None

1.1.7 discovery targeted-Hello

Use this command to set the holdtime or interval for the extended peer Hello message. Use the **no** form of this command to restore the default value.

discovery targeted-Hello {**holdtime|interval**} *seconds*

no discovery targeted-Hello {**holdtime|interval**}

Parameter description

Parameter	Description
holdtime	The holdtime of the Hello message for the extended mechanism.
interval	The interval of the Hello message for the extended mechanism.
seconds	Range within 1-65535

Default configuration

By default, the holdtime of the Hello message for the extended mechanism is 45s, and the interval of the Hello message is 5s, which is 1/9 of the holdtime.

Command mode

config-mpls-router mode

Usage guidelines

For the actual configuration, it is necessary to ensure the holdtime of the target Hello is larger than the interval value. Otherwise, LDP can not work normally according to the requirement. Note that this command is valid for the targeted Hello used by the extended discovery mechanism only.

Examples

```
DES-7200(config)# mpls route ldp
DES-7200(config-mpls-router)# discovery target-Hello holdtime 90
```

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute

1.1.8 explicit-null

Use this command to configure the distribution of explicit null labels to direct routes or direct route prefixes meeting specified ACL rules, or the distribution of explicit null labels to only the neighbors meeting rules and of implicit null labels to other neighbors. Use the **no** form of this command to cancel relevant configurations.

explicit-null [for *prefix-acl*] [to *peer-acl*]

no explicit-null

Parameter description

Parameter	Description
for *prefix-acl*	(Optional) Specify the prefixes of direct routes whose implicit null labels are replaced with explicit null labels.
to *peer-acl*	(Optional) Specify the LDP peers whose implicit null labels can be replaced by explicit null labels.

Default configuration

By default, implicit null labels are distributed to direct routes for all peers.

Command mode	**config-mpls-router** mode

Usage guidelines

Caution

1. When the LSP of the FEC to which a direct route corresponds serves as the bearer tunnel of an L2 VPN or an L3 VPN, an explicit null label cannot be distributed to the corresponding FEC of this direct route.
2. If a command to distribute explicit null labels is configured but no filtering rule is configured in the corresponding ACL, it is equivalent that the command is not configured, that is, implicit null labels are distributed to direct routes for all neighbors.
3. This command can be configured for global LDP instances only, and VRFs do not support this command.

Examples

If no parameter is specified, it indicates that explicit null labels are distributed to all direct routes by LDP:

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# explicit-null
```

The following command configures LDP to distribute explicit null labels to LDP peer 1.1.1.1 for direct routes with 192.168.0.0/16 as the prefix. Otherwise, the LDP distributes implicit null labels.

```
DES-7200(config)#ip access-list standard fec_acl
DES-7200(config-std-nacl)#permit 192.168.0.0 0.0.255.255
DES-7200(config-std-nacl)#exit
DES-7200(config)#ip access-list standard peer_acl
DES-7200(config-std-nacl)#permit host 1.1.1.1
DES-7200(config-std-nacl)#exit
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# explicit-null for fec_acl to peer_acl
```

Related commands

Command	Description
-	-

Platform description

None

1.1.9 graceful-restart

Use this command to enable the graceful restart (GR) capability of LDP. Use the **no** form of this command to disable the GR capability of LDP.

graceful-restart

no graceful-restart

Parameter description

Parameter	Description
no	Disable the GR capability of LDP.

Default configuration

By default, the GR capability of LDP is disabled.

Command mode

config-mpls-router mode

Usage guidelines

Use this command to enable the GR capability of LDP as follows:

- If a dual-engine device is enabled with the GR capability of LDP, traffic can be forwarded uninterruptedly and MPLS forwarding state can be consistent before and after restart when the master management board of the device becomes faulty or master/slave switchover is performed manually.
- By default, the GR capability is disabled on either of devices acting as GR-Restarter and GR-Helper.

Note

The LDP session must be restarted to make the GR capability of LDP take effect.

Examples

The following command enables the GR capability of LDP:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

	DES-7200(config)#**mpls router ldp** DES-7200(config-mpls-router)#**graceful-restart**

Related commands	**Command**	**Description**
	show mpls ldp graceful-restart	Show the LDP GR session and its parameters.
Platform description	None	

1.1.10 graceful-restart timer neighbor-liveness

Use this command to configure the survival time for an LDP neighbor. Use the **no** form of this command to restore the default value.

graceful-restart timer neighbor-liveness *seconds*

no graceful-restart timer neighbor-liveness

Parameter description	**Parameter**	**Description**
	seconds	Configure the survival time for an LDP neighbor, ranging from 5s to 300s.
	no	Restore the default value.

Default configuration	By default, the survival time for an LDP neighbor is 120s.
Command mode	**config-mpls-router** mode

Usage guidelines

Use this command to configure the survival time for an LDP neighbor as follows:

- The device uses this value only when it acts as a GR-Helper.
- When a device acts as a GR-Helper, it selects the smaller value of the configured neighbor-liveness time and the received reconnect time to enable the survival timer and keeps "old" entries before the survival timer times out.

Note

The LDP session must be restarted to make the survival time for an LDP neighbor take effect.

Examples

The following command configures the survival time for an LDP neighbor as 200s:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#graceful-restart
DES-7200(config-mpls-router)#graceful-restart timer
neighbor-liveness 200
```

Related commands

Command	Description
show mpls ldp graceful-restart	Show the LDP GR session and its parameters.

Platform description

None

1.1.11 graceful-restart timer reconnect

Use this command to configure the LDP session reconnect time. Use the **no** form of this command to restore the default value.

graceful-restart timer reconnect *seconds*

no graceful-restart timer reconnect

Parameter

Parameter	Description

description

seconds	Configure the LDP session reconnect time, ranging from 30s to 600s.
no	Restore the default value.

Default configuration

By default, the LDP session reconnect time is 300s.

Command mode

config-mpls-router mode

Usage guidelines

Use this command to configure the LDP session reconnect time as follows:

- During GR, both of devices acting as GR-Restarter and GR-Helper use the LDP session reconnect time.
- For the GR-Restarter, the LDP session reconnect time is used to keep "old" entries time.
- The GR-Helper selects the smaller value of the configured neighbor-liveness time and the received reconnect time to enable the survival timer and keeps "old" entries before the survival timer times out.

Note

The LDP session must be restarted to make the LDP session reconnect time take effect.

Examples

The following command configures the LDP neighbor reconnect time as 400s:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#graceful-restart
DES-7200(config-mpls-router)#graceful-restart timer reconnect 400
```

Related commands	**Command**	**Description**
	show mpls ldp graceful-restart	Show the LDP GR session and its parameters.
Platform description	None	

1.1.12 graceful-restart timer recovery

Use this command to configure the LDP session recovery time. Use the **no** form of this command to restore the default value.

graceful-restart timer recovery *seconds*

no graceful-restart timer recovery

Parameter description	**Parameter**	**Description**
	seconds	Configure the LDP session recovery time, ranging from 15s to 600s.
	no	Restore the default value.

Default configuration	By default, the LDP session recovery time is 120s.
Command mode	**config-mpls-router** mode

Usage guidelines

Use this command to configure the LDP session recovery time as follows:

- The device uses this value only when it acts as a GR-Helper.
- When a device acts as a GR-Helper, it selects the smaller value of the configured recovery time and the received recovery time to enable the recovery timer and keeps "old" entries before the recovery timer times out.

Note

The LDP session must be restarted to make the LDP session recovery time take effect.

Examples

The following command configures the LDP session recovery time as 200s:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#graceful-restart
DES-7200(config-mpls-router)#graceful-restart timer recovery 200
```

Related commands

Command	Description
show mpls ldp graceful-restart	Show the LDP GR session and its parameters.

Platform description

None

1.1.13 label-merge

Use this command to enable global label merge. Use the **no** form of this command to disable this function.

[**no**] **label-merge**

Default configuration

Enabled.

Command mode	**config-mpls-router** mode.
Usage guidelines	In the DU advertise control mode, label merge cannot be disabled. This command configuration resets the LDP session.
Examples	`DES-7200(config)# mpls route ldp` `DES-7200(config-mpls-router)# label-merge`

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute
mpls ldp distribution-mode	Configure the label distribution mode used for each interface.

1.1.14 label-retention-mode

Use this command to set the label retention mode. Use the **no** form of this command to restore the default value.

label-retention-mode {liberal | conservative}

[no] label-retention-mode

Parameter description

Parameter	Description
liberal	Use the liberal label retention mode
conservative	Use the conservative label retention mode

Default configuration	Use the liberal label retention mode

Command mode	**config-mpls-router** mode
Usage guidelines	Use this command to reset and rebuild the LDP session.
Examples	DES-7200(config)# **mpls route ldp** DES-7200(config-mpls-router)# **label-retention-mode liberal**

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute

1.1.15 label-switching

When the MPLS multi-service card is used to forward the MPLS service, use this command to enable the interface to process the MPLS label message.

[**no**] **label-switching**

Default configuration	For the equipment which uses the MPLS multi-service card to forward the MPLS service, its interface can not process the MPLS label message by default.
Command mode	Interface configuration mode.
Usage guidelines	This command is valid only for the equipment which uses the MPLS multi-service card(7200-ASE3) to forward the MPLS service.
Examples	DES-7200(config)# **interface Gi4/1** DES-7200(config-if)# **label-switching**

Related commands

Command	Description
show mpls label-pool	Show the usage of the label pool in each label space

1.1.16 ldp router-id

Use this command to set the router ID of the LDP. Use the **no** form of this command to restore the default value, which does not take effect immediately.

ldp router-id { *ip-address* | interface *interface-name* [force]}

no ldp router-id

Parameter description

Parameter	Description
ip-address	Specify a static IP address as the router ID of LDP. It takes effect immediately after being configured.
interface-name [**force]**	Configure the primary address of a specified interface as the router ID of LDP. If the **force** keyword is specified, the new router ID is forced to take effect immediately. Otherwise, the new router ID will not take effect immediately.

Default configuration

Use the system router ID as the LDP router ID.

Command mode

config-mpls-router mode

Usage guidelines

If a static IP address is specified as the router ID of LDP and the address takes effect immediately after being configured, it indicates that the established session is disconnected and that a new router ID is used to re-establish a session.

If the IP address of a specified interface is specified as the router ID of LDP and the **force** keyword is not carried, the primary address of the currently configured interface is used as the new router ID only when the currently used router ID is unavailable. To use the address of an interface as the router ID, the following conditions must be met:

(1) The VRF to which the interface belongs must be the same as that to which LDP belongs.

(2) The interface must be in Up state.

Otherwise, the router ID cannot take effect even if the **force** keyword is specified. The router ID takes effect only when the preceding conditions are met (in the case that the **force** keyword is specified).

If a configured static IP address replaces a configured interface address to act as the router ID of LDP or vice versa, the router ID takes effect immediately. In this case, the LDP sessions established under the LDP instance are disconnected automatically and then re-established.

It is recommended to use an interface address as the router ID of LDP. The purpose of using a static address is mainly to be compatible with commands of earlier versions.

Examples

```
DES-7200(config)# mpls router ldp

DES-7200(config-mpls-router)# ldp router-id interface vlan 10 force
```

Related commands

Command	Description
show mpls ldp parameter	Show all LDP configuration parameters under all or specified VRFs.

1.1.17 loop-detection

Use this command to enable loop detection. Use the **no** form of this command to disable loop detection.

[**no**]**loop-detection**

Default configuration	Disabled.
Command mode	**config-mpls-router** mode
Usage guidelines	Use this command to reset and rebuild the LDP session.
Examples	`DES-7200(config)# mpls router ldp` `DES-7200(config-mpls-router)# loop-detection`

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute
mpls ldp max-path-vector	Configure the maximum path vector allowed for LDP loop detection
mpls ldp max-hop-count	Configure the maximum hop count allowed for LDP loop detection

1.1.18 lsp-control-mode

Use this command to set the LDP control mode globally. Use the **no** form of this command to restore the default value.

lsp-control-mode [**independent** | **ordered**]

no lsp-control-mode

Parameter description

Parameter	Description
independent	Use the independent control mode
ordered	Use the ordered control mode

Default configuration	Independent control mode
Command mode	**config-mpls-router** mode
Usage guidelines	Use this command to reset and rebuild the LDP session.
Examples	`DES-7200(config)# mpls router ldp` `DES-7200(config-mpls-router)# lsp-control-mode ordered`

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute

1.1.19 mpls ip (Global configuration mode)

Use this command to enable the MPLS forward in the global configuration mode. Use the **no** form of this command to disable MPLS forward.

[no] mpls ip

Default configuration	The MPLS forward is not enabled.
Command mode	Global configuration mode.

Usage guidelines	To implement the mpls forward, it is necessary to enable the MPLS globally firstly. This command is invalid for the mpls forward on the switch. After the mpls forward is disabled by the process forward, the switch can not send and receive the MPLS messages.

Examples	`DES-7200(config)# mpls ip`

Related commands	

Command	Description
mpls ip	Enable the MPLS in the interface configuration mode.

1.1.20 mpls ip (Interface configuration mode)

Use this command to enable the MPLS forward and the LDP functions in the interface configuration mode. Use the no form of this command to disable the LDP function to terminate the MPLS forward.

[**no**] **mpls ip**

Default configuration	Disabled.

Command mode	Interface configuration mode.

Usage guidelines	For the interface which doesn't use the MPLS multi-service card to forward the MPLS service, the MPLS forward function is disabled by default. Therefore, you must use this command to enable the MPLS forward function, and the LDP function on the interface is enabled automatically at the same time. If the LDP function is not enabled on this interface, it can not use the LDP to set up the LSP. It only allows enable the MPLS function on the L3 interface.

Examples

```
DES-7200(config)# interface Gi4/1
DES-7200(config-if)# mpls ip
```

Related commands

Command	Description
mpls ldp Hello-interval	Configure the interval for sending Hello messages
mpls ldp Hello-holdtime	Configure the Hello packet holdtime

1.1.21 mpls ip fragment

Use this command to set the processing if it exceeds the MPLS MTU after the IP message is encapsulated with the MPLS label.

[no] mpls ip fragment

Default configuration

After the entered IP packet is encapsulated with the MPLS label, if its size exceeds the defined size of the MPLS MTU, it will carry out the fragment to the original IP packet before the MPLS label is encapsulated to send.

Command mode

Global configuration mode.

Usage guidelines

This command is valid only for the process forward. Use the **no mpls ip fragment** command to disable the fragment function for process forward. Namely, it will be discarded directly if its size exceeds the defined size of the MPLS MTU after the entered IP packet is encapsulated with the MPLS label.

Examples

```
DES-7200(config)# no mpls ip fragment
```

Related

Command	Description

	mpls ip	Enable MPLS globally.

1.1.22 mpls ip icmp-error pop

Use this command to set the processing mode for ICMP error packets during the forwarding of MPLS packets.

mpls ip icmp-error pop *labels*

no mpls ip icmp-error pop

Parameter description

Parameter	Description
labels	Number of labels for packets to be processed

Default configuration

By default, the generated ICMP error packet continues to be forwarded along the original LSP after being labeled with the original tag.

Command mode

Global configuration mode

Usage guidelines

By default, the generated ICMP error packet continues to be forwarded along the original LSP until to the LSP egress. At the egress, the packet is rerouted and forwarded according to the inner IP address after its label stack is removed. You can use this command to change this default action by configuring packets with different numbers of labels to be processed differently. When the number of labels of a forwarded packet is less than or equal to the configured value, the ICMP error packet directly uses the IP route forwarding table of the FEC to which the top label corresponds.

Examples

```
DES-7200(config)# mpls ip icmp-error pop 2
```

Related

Command	Description

	mpls ip	Enable MPLS globally.

Platform description	None

1.1.23 mpls ip ttl propagate

Use this command to enable or disable the IP TTL copy function of the MPLS.

mpls ip ttl propagate {**public** | **vpn**}

no mpls ip ttl propagate {**public** | **vpn**}

	Parameter	**Description**
Parameter description	**public**	Specify whether to enable TTL copy function or not for the sending messages.
	vpn	Specify whether to enable TTL copy function or not for the forwarding messages.

Default configuration	By default, it enables TTL copy function for both the sending and forwarding messages.

Command mode	Global configuration mode

Usage guidelines

The following are two modes of MPLS TTL:

- TTL copy mode: it is the default working mode. In this mode, the pushed label TTL is copied from the TTL of the existed header of the IP packet or the MPLS packet when Pushing the label. The TTL of the inner IP packet or the MPLS packet is copied from the TTL of the outer label when Popping the label.
- TTL non-copy mode: in this mode, set the value of pushed label TTL to 255 when Pushing the label and keep the value of the TTL of the inner IP packet or the MPLS packet when Popping the label.

Caution:

After the TTL copy is enabled, the TTL of the inner header is not copied but retained if it is smaller than the TTL of the outer header.

For the switch products, the TTL of the inner header is directly copied from the outer header during the PHP Pop operation, if TTL copy is enabled. The TTL of the packets forwarded, however, does not decrease by one. If TTL non-copy is enabled, the TTL of the inner header does not copy that from the outer header. Instead, the TTL of the inner header is retained. The TTL of packets forwarded also does not decrease by one.

Examples

The following example disables the TTL copy function of the forwarding message:

```
DES-7200(config)# mpls ip ttl propagate public
```

Related commands

Command	Description
mpls ip	Enable MPLS globally.

1.1.24 mpls ldp distribution-mode

Use this command to set the label distribution mode used by LDP on each interface. Use the **no** form of this command to restore the default value.

mpls ldp distribution-mode {**dod | du**}

no mpls ldp distribution-mode

Parameter description

Parameter	Description
dod	Use the downstream on-demand distribution mode
du	Use the downstream active distribution mode

Default configuration

Use the downstream active distribution mode.

Command mode

Interface configuration mode.

Usage guidelines

If the interconnected LDP sessions use different distribution modes, the du mode will be used forcibly for both of them. Use this command to reset and rebuild the LDP session.

Examples

```
DES-7200(config)# interface vlan 10
DES-7200(config-if)# mpls ldp distribution-mode dod
```

Related commands

Command	Description
loop detection-mode	Configure loop detection

1.1.25 mpls ldp frr nexthop

Use this command to enable the LDP FRR function on an interface. Use the **no** form of this command to disable the LDP FRR function.

mpls ldp frr nexthop nexthop-address [interface interface-type interface-number] [acl acl-name] [priority priority]
no mpls ldp frr nexthop {* | *nexthop-address* [**interface** *interface-type interface-number*] [**acl** *acl-name*] [**priority** *priority*]}

Parameter description

Parameter	Description
nexthop *nexthop-address*	Specify the next hop IP address of a backup port.
interface *interface-type interface-number*	Configure the interface type and interface number.
acl *acl-name*	The FEC that matches the IP prefix defined with the name of a specified ACL can generate a backup LSP.
priority *priority*	Specify the priority of a backup LSP. The smaller the priority value, the higher the priority of a backup LSP. The priority vlaue is an integer, ranging from 1 to 65535, 10 by default.
nexthop *	Indicates all next hop IP addresses, namely all backup ports.
no	Mean disabling the LDP RFF function.

Default configuration

By default, the LDP FRR function is disabled.

Command mode

Interface configuration mode

Usage guidelines

This command is used to configure the LDP FRR function on an interface and generate a backup LSP by specifying a backup port:

- When the address of the backup port is borrowed or lent, the interface type and interface number must be specified.
- To configure the LDP FRR function on an interface, the specified backup port must be under one VRF with the current interface, which cannot be specified as the backup port.
- If the LDP FRR function is configured on an interface, the LDP FRR configuration on the interface is automatically deleted when

the backup port is deleted.

- Multiple backup ports can be configured on one interface and distinguished by priority. If the next hop IP address of a backup port is specified on an interface but the priority is not specified, the default priority is adopted. If the next hop IP addresses of backup ports are specified on one interface but priorities are not specified, the subsequent configuration overwrites the preceding configuration and default priorities are adopted, that is, only one backup port is configured on this interface.
- There can be a maximum of 10 backup ports with 10 different priorities on an interface, but only one backup port is elected as the effective one. If the effective backup port becomes faulty, the system re-elects another effective backup port from configured backup ports according to priorities.
- You can configure an ACL rule for the FEC of routes with the same next hop on one interface.
  - LDP FRR can only process standard ACLs, that is, ACLs created by using the **ip access-list standard** command.
  - If no ACL rule is specified, LDP FRR attempts to establish an LSP on the path specified by *nexthop-address* for all FECs passing an interface.
  - If an ACL rule is specified and there are both Permit items and Deny items in the ACL rule, a backup LSP can be established on the path specified by *nexthop-address* for only the LSP to which the FEC permitted by the interface corresponds.
  - The ACL rule name is specified when LDP FRR is configured. However, if the user does not create an ACL rule (that is, no ACL rule exists), the system performs Deny operations to all FECs passing an interface, that is, the system does not establish LSPs for all FECs passing an interface.

Caution

In configuring LDP FRR, you must configure the label to work in free retention mode.

Note

During LDP GR, the LDP FRR function cannot be enabled or disabled.

Examples

The following example enables the LDP FRR function on GE0/1 of the switch. The next hop IP address of the backup port is 5.5.51.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface GigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#label-switching
DES-7200(config-if-GigabitEthernet 0/1)#mpls ip
DES-7200(config-if-GigabitEthernet 0/1)#exit
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#exit
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#mpls ldp frr nexthop 5.5.5.1
```

Related commands

Command	Description
show mpls rib	View MPLS routing information.

Platform description

None

1.1.26 mpls ldp frr timer protect-time

Use this command to configure the time of the LDP FRR protection timer for controlling the time used for the slave link to switch as the master link, with second as the unit. Use the **no** form of this command to restore the default value.

mpls ldp frr timer protect-time {infinity | *seconds*}

no mpls ldp frr timer protect-time

Parameter description

Parameter	Description
infinity	When the LSP link returns to normal, its traffic will not be transferred to the master LSP link for ever.
seconds	Indicates the time of protection timer. The value is an integter, ranging form 0 to 65535s.

	no	Restore the default vlaue of 10s.

Default configuration

By default, the time of protection timer is 10s. It indicates that, within this time, if the master LSP link recovers from the fault, the traffic is transferred to the master LSP link when the protection timer times out.

Command mode

Interface configuration mode

Usage guidelines

If the time of the LDP FRR protection timer is configured, the system does not transfer the service traffic to the master link immediately after the master link recovers from the fault. Instead, the system transfers the service traffic to the master link after the LDP FRR protection timer times out, thus preventing switchover of traffic on the master/slave links caused by Up/Down oscillation.

Caution

1. In the following cases, Up/Down oscillation can be suppressed for the reason that the routing protocol is not aware of the change in the next hop immediately after link fault recovery.

(1) The master LSP link uses BFD and OSPF but is not configured with cooperation between BFD and OSPF.

(2) The master LSP link uses BFD and a protocol other than OSPF.

2. In the following cases, Up/Down oscillation cannot be suppressed for the reason that the routing protocol is aware of the change in the next hop immediately after link fault recovery.

(1) The master LSP link uses BFD and OSPF and is configured with cooperation between BFD and OSPF.

(2) The master LSP link uses interface detection.

Examples

The following example enables LDP on GE0/1 of the switch and configures backup LSP protection time for this interface:

```
DES-7200#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# mpls ip
DES-7200(config)#interface GigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#label-switching
DES-7200(config-if-GigabitEthernet 0/1)#mpls ip
DES-7200(config-if-GigabitEthernet 0/1)#exit
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)#exit
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#mpls ldp frr protect-time 15
```

Related commands

Command	Description
mpls ldp frr nexthop	Enable the LDP FRR function on the interface.

Platform description

None

1.1.27 mpls ldp hello-holdtime

Use this command to configure the holdtime in seconds for LDP Hello packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp hello-holdtime *seconds*
no mpls ldp hello-holdtime

Parameter description

Parameter	Description
seconds	Holdtime of Hello messages, ranging from 1s to 65535s. Holdtime 65535 indicates that the Hello message will never time out.

Default configuration

15 seconds

Command mode	Interface configuration mode.
Usage guidelines	This command is valid only for the LDP Link Hello packets for the basic discovery mechanism and may lead to a change in the interval for sending Hello messages. Use the **discovery targeted-Hello** command to set the Hello interval for the exteded discovery mechanism.

Examples	The following command configures the Link Hello holdtime of LDP on an interface as 30s:
	`DES-7200(config)# interface vlan 10`
	`DES-7200(config-if)# mpls ldp Hello-holdtime 30`

Related commands

Command	Description
mpls ldp Hello-interval	Configure the interval for sending Hello messages.
discovery targeted-Hello	Configure the interval and timeout time of sending Hello messages for the extended discovery mechanism.

1.1.28 mpls ldp hello-interval

Use this command to configure the holdtime in seconds for LDP Hello packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp Hello-interval *seconds*

no mpls ldp Hello-interval

Parameter description

Parameter	Description
seconds	Interval for sending Hello messages, ranging from 1s to 65535s.

Default configuration	5 seconds
Command mode	Interface configuration mode.
Usage guidelines	The interval for sending Link Hello packets on an interface may not be consistent with that configured by this command. (1) By default, if the minimum holdtime among all holdtimes negotiated with neighbors an interface is less than 15s, the actually used interval for sending Hello packets is 1/3 of the minimum holdtime and 1s minimum. (2) By default, if the minimum holdtime among all holdtimes negotiated with neighbors of an interface is greater than or equal to 15s, the actually used interval for sending Hello packets is 5s. (3) If the configured interval is greater than 1/3 of the minimum value among all holdtimes negotiated with neighbors of an interface, the actually used interval for sending Hello packets is 1/3 of the minimum holdtime and 1s minimum. (4) If the configured interval is less than 1/3 of the minimum value among all holdtimes negotiated with neighbors of an interface, the configured interval for sending Hello packets is used. In the actual configuration, this value must be less than the value of Hello-holdtime. This command is valid only for the LDP Link Hello packets for the basic discovery mechanism. Use the **discovery targeted-Hello** command to set the Hello holdtime for the extended discovery mechanism.

Examples	The following command configures the interval for sending Hello packets as 10s:
	`DES-7200(config)# interface vlan 10`
	`DES-7200(config-if)# mpls ldp Hello-interval 10`

Related

Command	Description

mpls ldp hello-holdtime	Configure the Hello packet holdtime in seconds.
discovery targeted-hello	Configure the interval and timeout time of sending Hello messages for the extended discovery mechanism.

1.1.29 mpls ldp keepalive-holdtime

Use this command to configure the holdtime for keepalive packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp keepalive-holdtime *seconds*

no mpls ldp keepalive-holdtime

Parameter description

Parameter	Description
seconds	Holdtime of keepalive packets, ranging from 15s to 65535s

Default configuration

45 seconds

Command mode

Interface configuration mode.

Usage guidelines

This command is valid for the LDP sessions to be created instead of created LDP sessions. This command has no influence on the LDP session set up by the extended discovery mechanism. Use the **targeted-session holdtime** command to modify the Keepalive Holdtime of the LDP session set up by the extended discovery mechanism.

Examples

The following command configures the holdtime of the Keepalive packet of LDP on an interface as 90s:

```
DES-7200(config)# interface vlan 10
DES-7200(config-if)# mpls ldp keepalive-holdtime 90
```

Related commands

Command	Description
targeted-session holdtime	Set the holdtime of Keepalive packets for the extended mechanism.

1.1.30 mpls ldp max-hop-count

Use this command to configure the maximum hop count allowed for loop detection on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-hop-count *number*

no mpls ldp max-hop-count

Parameter description

Parameter	Description
number	Maximum hop count allowed for loop detection, ranging from 1 to 255

Default configuration

The default value is 254.

Command mode

Interface configuration mode.

Usage guidelines

The value configured by this command is valid only after loop detection is configured. If the hop count value in the label mapping message or the label request message of LDP is greater than the configured value, it is deemed that a loop occurs. This command is invalid for the label mapping message and label request message received previously, but valid for those received later.

Examples

The following command configures the LDP hop count of the interface as 30:

```
DES-7200(config)# interface vlan 10
```

```
DES-7200(config-if)# mpls ldp max-hop-count 30
```

Related commands

Command	Description
loop-detection	Configure LDP loop detection

1.1.31 mpls ldp max-label-requests

Use this command to configure the maximum label requests allowed on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-label-requests *times*

no mpls ldp max-label-requests

Parameter description

Parameter	Description
times	Maximum request times, ranging from 0 to 255

Default configuration

There is no limit by default, indicating that label requests are retransmitted until a label mapping message is received.

Command mode

Interface configuration mode.

Usage guidelines

This command is invalid for the label request times in the created LDP session on the interface, and valid for newly-created LDP sessions. The value 0 means that the label request will not be retransmitted.

Examples

The following command configures the maximum number of label requests of LDP allowed on an interface as 5:

```
DES-7200(config)# interface vlan 10
DES-7200(config-if)# mpls ldp max-label-requests 5
```

Related commands

Command	Description
mpls ldp distribution-mode	Configure the label distribution mode.

1.1.32 mpls ldp max-path-vector

Use this command to configure the maximum path vector value allowed for loop detection on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-path-vector *number*

no mpls ldp max-path-vector

Parameter description

Parameter	Description
number	Maximum path vector value, ranging from 0 to 255.

Default configuration

The default value is 254.

Command mode

Interface configuration mode.

Usage guidelines

The configured path vector value takes effect only after the LDP instance enables loop detection. If the number of LDR IDs contained in the path vector list of the label mapping message or the label request message of LDP is greater than the configured maximum path sector value, it is deemed that a loop occurs. This command is invalid for the created LDP sessions, but influences the LDP sessions to be created.

Examples

The following command configures the maximum path vector value of LDP on an interface as 10:

```
DES-7200(config)# interface vlan 10
DES-7200(config-if)# mpls ldp max-path-vector 10
```

Related commands

Command	Description
loop-detection	Set LDP loop detection.

1.1.33 mpls ldp max-pdu

Use this command to configure the maximum PDU value. Use the **no** form of this command to restore the default value.

mpls ldp max-pdu *max-pdu*

no mpls ldp max-pdu

Parameter description

Parameter	Description
max-pdu	The maximum PDU value in exchanging the LDP messages, in bytes, ranging from 256 to 4096

Default configuration

The default value is 4096.

Command mode

Interface configuration mode.

Usage guidelines

This command does not influence the created LDP session on the interface.

Examples

The following command configures the maximum length of LDP messages as 256:

```
DES-7200(config)# interface vlan 10
DES-7200(config-if)# mpls ldp max-pdu 256
```

1.1.34 mpls ldp transport-address

Use this command to set the transport address used by basic LDP sessions. Use the **no** form of this command to restore the default value.

mpls ldp transport-address {interface | *ip-address*}

no mpls ldp transport-address

Parameter description

Parameter	Description
interface	The LDP session uses the main address of an interface itself.
ip-address	The LDP session uses an IP address specified by this parameter.

Default configuration

Use the LSR ID of LDP as the transport address.

Command mode

Interface configuration mode.

Usage guidelines

This command is ineffective to LDP sessions created by the extended discovery mechanism, and it is effective only to LDP sessions created by the basic discovery mechanism. When this interface transport address is configured, this command is ineffective to the LDP sessions that have been created by basic discovery mechanism, and effective to newly created sessions.

Examples

The following example configures basic LDP sessions to use the main address of an interface as the transport address:

```
DES-7200(config)# interface vlan 10

DES-7200(config-if)#mpls ldp transport-address interface
```

Related commands

Command	Description
show mpls ldp parameters	Show the LDP parameters under all or specified VRFs.
transport-address	Globally configure the transport address used by basic LDP sessions.

Platform description

None

1.1.35 mpls mtu

Use this command to configure the mtu value when the MPLS messages are forwarded.

mpls mtu *mtu*

no mpls mtu

Parameter description

Parameter	Description
mtu	The length of label packets supported by the interface, in bytes, ranging from 64 to 1500

Default configuration

The MPLS mtu value equals to the interface mtu.

Command mode

Interface configuration mode.

Usage guidelines	By default, the mtu of the transmittable MPLS label packet on an interface is equal to default the interface mtu. The MPLS mtu determines whether to fragment the MPLS packet during the message sending. The length of the MPLS mtu includes the total length of the MPLS encapsulating and encapsulated (IP) layers. The MPLS mtu on the interface must not exceed the actual transmssion capability of the interface. This command is valid for process forwarding and router fast forwarding only instead of switches adopting ASIC forwarding. The switch forwards the packets according to the actually configured mtu on the interface and discards the packets that exceed the confgured mtu. Use the **mtu** command in interface configuration mode to adjust the mtu on the interface. In actual forwarding, you should try to prevent forwarding performance from degrading due to fragmenting by adjusting the mtu value.

Examples

```
DES-7200(config)# interface Gi4/1
DES-7200(config-if)# mpls mtu 1510
```

Related commands

Command	Description
mpls ip	Enable the MPLS globally.

1.1.36 mpls router ldp

Use this command to enable LDP, use the **no** form of this command to disable LDP.

[no] mpls router ldp [*vrf-name***]**

Default configuration	Disabled
Command mode	Global configuration mode.

Usage guidelines	The number of LDP instances is limited by the number of VRFs on a device. Each VRF can start one LDP instance. If no VRF is enabled, LDP of the global VRF is enabled or disabled by default.

Examples

The following command is used to enable LDP of the global VRF and enter LDP configuration mode:

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface vlan 10 force
```

The following command is used to enable LDP of vpna and enter LDP configuration mode:

```
DES-7200(config)# mpls router ldp vpna
DES-7200(config-mpls-router)# ldp router-id interface vlan 10 force
```

1.1.37 mpls static ftn

Use this command to allow you to add one FTN entry to the global FTN table. Use the **no** form of this command to delete the specified FTN entry from the FTN table.

mpls static ftn *ip-address/mask* **out-label** *label* **nexthop** *interface-name nexthop-ip*

no mpls static ftn *ip-address//mask*

Parameter description

Parameter	Description
ip-address//mask	Corresponding FEC, namely the destination address.
out-label *label*	Corresponding outgoing label of this FEC.
nexthop *interface-name* *nexthop-ip*	The next hop of this FEC, including the egress and the IP address of the next hop.

Command mode	Global configuration mode.

Usage guidelines	This command allows you to add an FTN entry to the global FTN table. After the router with MPLS enabled receives an IP packet, it looks up for the next hop in the FTN table according to the destination address of the IP packet by maximum match. If the next hop is found, it performs label forwarding to the IP packet. For the FTN whose destination address and mask are both 0, it is valid only when this default route exists in the IP route forwarding table.
Examples	`DES-7200(config)# mpls static ftn 192.168.0.0/16 out-label 100 nexthop gi4/1 10.10.10.1`

Related commands

Command	Description
show mpls forwarding-table	Show the overview information of the global FTN table

1.1.38 mpls static l3vpn-ftn

Use this command to add the FTN of one L3 VPN. Use the **no** form of this command to delete this FTN.

mpls static l3vpn-ftn *vrf-name ip-address/mask* **out-label** *label* **remote-pe** *ip-addr*

mpls static l3vpn-ftn *vrf-name ip-address/mask* **local-forward nexthop** *interface-name nexthop-ip*

no mpls static l3vpn-ftn *vrf ip-address/mask*

Parameter description

Parameter	Description
vrf-name	Specify the name of the VRF whose FTN table to which the FTN entry is to be added
ip-address/mask	Fec, namely the destination network.
out-label *label*	It indicates that the corresponding private network FTN should reach to other PE forwarding through the LSP tunnel. At the same time, it will be specified with the private network label used for the forward.
remote-pe *ip-addr*	The address of the egress PE.

	local-forward nexthop *interface-name nexthop-ip*	It indicates that the corresponding private network FTN will be forwarded to the next hop by this PE directly. At the same time, it will specify the egress of the next hop and the IP address.

Command mode	Global configuration mode.
Usage guidelines	This command allows you to add an FTN entry to the FTN table specified by the vrf-name. After the router with MPLS enabled receives an IP packet, it looks up for the next hop in the FTN table according to the destination address of the IP packet according to maximum match. If the next hop is found, it performs label forwarding to the IP packet. For the FTN whose destination and mask is 0, it is valid only when this route exists in the IP route forwarding table.
Examples	`DES-7200(config)# mpls static l3vpn-ftn 192.168.0.0/16 out-label 100 remote-pe 10.10.10.1`

Related commands

Command	Description
show mpls forwarding-table	Show the overview information of the global FTN table

1.1.39 mpls static l2vc-ftn

Use this command to configure one static VC FTN item. Use the **no** form of this command to delete the configured FTN item.

mpls static l2vc-ftn *vc-id vc-peer-ip* **out-label** *label*

no mpls static l2vc-ftn *vc_id vc_peer_ip*

Parameter description

Parameter	Description
vc-id	The id of the VC instance.

	vc-peer-ip	The IP address at another PE of Vc.
	out-label *label*	Used for the private network egress label when this VC FTN is forwarded.

Command mode	Global configuration mode.
Usage guidelines	This command is used to create one ftn item for the vc instance. After the frame is received from the AC binding with this VC, it will be stamped with the private network label for the data frame according to the content of this ftn item, and find the LSP that reaches the peer PE according to the vc peer ip, and then forward the frame.
Examples	`DES-7200(config)# mpls static l2vc-ftn 1 10.10.10.1 out-label 21`

Related commands

Command	Description
show mpls l2vc ftn-table	Show the ftn table item of all VC instances.
show mpls forwarding-table	Show the forwarding table item of the MPLS.

1.1.40 mpls static ilm in-label

Use this command to add one ILM table item to the ILM table. Use the **no** form of this command to delete the configured ILM item.

mpls static ilm in-label *in-label* **forward-action swap-label** *label* **nexthop** *interface-name nexthop-ip* **fec** *ip-address/mask*

mpls static ilm in-label *in-label* **forward-action pop-l3vpn-nexthop** *vrf-name* **nexthop** *interface-name nexthop-ip* **fec** *ip-address/mask*

mpls static ilm in-label *in-label* **forward-action pop-l2vc-destport vc-id** *vc-peer-addr*

no mpls static ilm in-label *in-label*

Parameter description

Parameter	Description
in-label	The ingress label value of this ILM table item.
forward-action	Specify the forward behavior of this ILM table item. **swap-label:** apply to the ILM table item of the public network, to indicate the label switching and forwarding. **pop-l3vpn-nexthop:** apply to the ILM table item of the L3 VPN, to indicate the pop-up label, and forward it to the next hop of the specified VRF. **pop-l2vc-destport:** apply to the ILM table item of the L2 VPN, to indicate the pop-up label, and forward the message from the specified interface.
label	For the **swap-label** forward behavior, it will specify the egress label value of the switched label value.
vrf-name	For the **pop-l3vpn-nexthop** forward behavior, it will specify the VPN of the specified ILM, namely VRF.
Interface-name	For the **pop-l2vc-destport** forward behavior, it will specify the forwarded egress.
nexthop *interface-name nexthop-ip*	Specify the next hop, including the egress and the IP address of the next hop.
fec	Indicate this ILM is created for which FEC.
ip-address/mask	Correspond to the fec format of the global or **l3 vpn** application, to indicate one destination network.
vc-id	Correspond to the fec format of the **l2vpn** application, to indicate the VC instance.
vc-peer-addr	Address of the VC peer.

Command mode	Global configuration mode.
Usage guidelines	This command allows you to add an ILM entry to the ILM table. After the router with MPLS enabled receives an IP packet with label, it looks up for the next hop in the ILM table according to the label of the IP packet according to maximum match. If the next hop is found, it swaps, pops up the label of the IP packet or performs VPN forwarding after pop-up.
Examples	`DES-7200 (config)# mpls static ilm in-label 20 forward-action swap-label 30 nexthop gi4/2 10.10.10.1 fec 172.16.0.0/26`

Related commands

Command	Description
show mpls forwarding-table	Show the information of the MPLS forwarding table.

1.1.41 neighbor labels accept

Use this command to configure the LSR to filter label mapping messages for the LDP peer according to a specified ACL rule. Use the **no** form of this command to delete the corresponding rule.

neighbor *ip-address* labels accept *acl-name*
no neighbor *ip-address* labels accept

Parameter description

Parameter	Description
ip-address	Router ID of the peer LSR
acl-name	Name of the specified ACL rule

Default configuration	No filtering rule is configured by default.

Command mode

config-mpls-router mode.

Usage guidelines

This command is effective to only the IP route FEC instead of other FECs such as PW FEC. If this command is used to configure a flitering rule for incoming label mapping messages, label mapping messages of the FEC from a specified neighbor meeting the ACL rule can be received and those of other FECs from this neighbor are discarded. However, label mapping messages sent by other neighbors are not affected and are still received. If this command is configured for a neighbor but no filtering rule is configured for the corresponding ACL, label mapping messages of all FECs sent by this neighbor are discarded. When the rule is cancelled by using the **no** form of this command, label mapping messages that have been filtered are not affected (that is, messages that have been discarded cannot be recovered) and only label mapping messages received thereafter are affected. In this case, the **clear mpls ldp neighbor** command needs to be used to reset the LDP session. Only one rule can be configured for one neighbor. 从次配置的话，后面的配置将覆盖前面的。Each LDP instance can be used to configure filtering rules for a maximum of 64 neighbors.

Examples

In the following example, only label mapping messages of the FEC with 192.168.0.0/16 as the route prefix and sent from the neighbor 10.10.10.1 are received, and those of other FECs sent from this neighbor are not received.

```
DES-7200(config) #ip access-list standard fec_acl
DES-7200(config-std-nacl)#permit 192.168.0.0 0.0.255.255
DES-7200(config-std-nacl)# exit
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# neighbor 10.10.10.1 labels accept fec_acl
```

Related commands

Command	Description
clear mpls ldp neighbor	Forcibly disconnect the LDP session.

	show mpls ldp neighbor	Show the LDP session state.

Platform description	None

1.1.42 neighbor password

Use this command to enable MD5 authentication of LDP. Use the **no** form of this command to disable MD5 authentication of LDP.

neighbor *ip-address* password [0 | 7] *pwd-string*
no neighbor *ip-address* password

Parameter description

Parameter	Description
ip-address	Trasnport address of the peer LSR
[0 | 7]	(Optional) 0 means typing a key in plain text and 7 means typing a key in encrypted text. A key is typed in plain text by default.
pwd-string	Password string, which is case-sensitive. If the password string is entered in plain text, it is a string of 1 to 25 characters; if the password string is entered in encrypted text, it is a string of 1 to 52 characters.

Default configuration	MD5 authentication of LDP is disabled by default.
Command mode	**config-mpls-router** mode.

Usage guidelines

A key can be typed in either plain text or encrypted text. In the former case, if the **service password-encryption** command is used to enable the encryption service in global configuration mode, the key is saved in encrypted text when the current configuration is saved or viewed.

To enable LDP authentication function, the keys configured on both ends of the LDP peer need to be the same. The change to the key will cause disconnection of established LDP sessions and re-attempt to establish them.

If a router is configured with a key but the LDP peer on the other end is not configured with a key, the following will be prompted when the two ends attempt to establish a session:

%TCP-6-BADAUTH: No MD5 digest from 10.40.10.10(20836) to 10.10.10.10(646)

If the keys configured on both ends are not the same, the following will be prompted when the two ends attempt to establish a session:

%TCP-6-BADAUTH: MD5 digest failed for (10.20.10.10, 55998)->(10.10.10.10, 646)

Examples

The following example configures MD5 authentication to be adopted for sessions with 10.10.10.1, with the plain text key being 123456:

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# neighbor 10.10.10.1 password 123456
```

Related commands

Command	Description
show mpls ldp discovery	Show the information about neighbors discovered by LDP.
show mpls ldp neighbor	Show the LDP session state.
neighbor *ip-address*	Create an LDP extended peer.

Platform description

None

1.1.43 neighbor

Use this command to create an ldp extended peer. Use the **no** form of this command to delete the ldp extended peer.

[no] neighbor *ip-address*

Parameter description

Parameter	Description
ip-address	The Router ID of the peer LSR.

Default configuration

There is no LDP extended peer by default.

Command mode

config-mpls-router mode.

Usage guidelines

To set up an extended LDP session, the both ends of the LSR of the session to be built must be configured. It fails to set up the extended LDP session if the extended peer is configured at only one end.

Examples

The following command configures 10.10.10.1 as an extended peer of the LSR:

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# neighbor 10.10.10.1
```

Related commands

Command	Description
show mpls ldp discovery	Show the information of neighbors discovered by the LDP.
show mpls ldp neighbor	Show the LDP session state.

1.1.44 ping mpls

Use this command to detect the connectivity of an MPLS LSP.

ping mpls ipv4 *ip-address/mask* [repeat *repeat*] [ttl *time-to-live*] [timeout *timeout*] [size *size*] [interval *mseconds*] [source *ip-address*] [destination *ip-address*] [force-explicit-null] [pad *pattern*] [reply mode {ipv4 | router-alert}] [dsmap] [flags fec] [verbose]

Parameter description

Parameter	Description
ip-address/mask	IPv4 address and subnet mask length of the destination FEC to be tested
repeat *repeat*	(Optional) Number of times to resend an Echo Request packet, ranging from 1 to 2147483647, 5 by default
ttl *time-to-live*	(Optional) Specify the initial MPLS TTL value for sending packets, ranging from 1 to 255, 255 by default.
timeout *timeout*	(Optional) Specify the timeout time for packets, ranging from 0 to 3600, 2 by default.
size *size*	(Optional) Specify the size of packets, ranging from 84 to 18024, 84 by default.
interval *mseconds*	(Optional) Specify the minimum interval time (in milliseconds) between two consecutive Echo Request packets sent, ranging from 0 to 3600000, 0 by default
source *ip-address*	(Optional) Source address. It is the destination address when the peer sends an Echo Reply packet.
destination *ip-address*	(Optional) Specified 127/8 segment address. It is used to fill the IP header, 127.0.0.1 by default.
force-explicit-null	(Optional) Whether to forcibly add an explicit null label to the MPLS label. By default, it is not added.
pad *pattern*	(Optional) Pad pattern of packets, 0xABCD by default

reply mode {**ipv4** | **router-alert**}	(Optional) Specify the reply mode of the Echo Request packet: **ipv4**: reply with an IPv4 UDP packet (default) **router-alert**: reply with an IPv4 UDP packet with the Router Alert option
dsmap	(Optional) Require returning downstream information.
flags fec	(Optional) Set forcible FEC stack check.
verbose	(Optional) Show detailed information about Echo Reply packets. By default, the informaiton is not shown.

Default configuration

See the preceding parameter desription.

Command mode

Privileged mode

Usage guidelines

You can change some default parameter values by specifying optional parameters. In addition to the directly typed command, interactive typing mode is provided. You can enter the interactive typing mode by pressing **Enter** after typing the **ping mpls** command.

Examples

Example 1: To detect the connectivity from the local device to the LSP of 10.10.10.10/32, type the following command:

```
DES-7200# ping mpls ipv4 10.10.10.10/32 verbose
Sending 5, 84-byte MPLS Echoes to 10.10.10.10/32,
  timeout is 2 seconds, send interval is 0 msec:
    < press Ctrl+C to break >
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
 'L'-labeled output interface,'B'-unlabeled output interface,
 'D'-DS Map mismatch,'F'-no FEC mapping,'f'-FEC mismatch,
```

```
 'M'-malformed request,'m'-unsupported tlvs,'N'-no label entry,
 'P'-no rx intf label prot,'p'-premature termination of LSP,
 'R'-transit router,'I'-unknown upstream index,
 'X'-unknown return code,'x'-return code 0
Type escape sequence to abort.
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
Success rate is 100 percent(5/5),round-trip min/avg/max=20/36/60 ms
```

Example 2: To return downstream information, use the dsmap parameter and ttl parameter together (because if the egress LSR is reached, downstream information is not returned):

```
DES-7200# ping mpls ipv4 10.40.10.10/32 dsmap ttl 1
Sending 5, 84-byte MPLS Echoes to 10.4(2)0.10.10/32,
    timeout is 2 seconds, send interval is 0 msec:
      < press Ctrl+C to break >
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
 'L'-labeled output interface,'B'-unlabeled output interface,
 'D'-DS Map mismatch,'F'-no FEC mapping,'f'-FEC mismatch,
 'M'-malformed request,'m'-unsupported tlvs,'N'-no label entry,
 'P'-no rx intf label prot,'p'-premature termination of LSP,
 'R'-transit router,'I'-unknown upstream index,
 'X'-unknown return code,'x'-return code 0
Type escape sequence to abort.
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
```

```
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
Success rate is 0 percent (0/5)
```

Field	Description
!	A correct Reply packet is received, indicating that the LSP is connected.
Q	The Request packet is not sent, indicating that there is no LSP corresponding to the destination FEC on the local device.
.	The time to receive a Reply packet times out, indicating that no Reply packet is received within a specified period of time.
L	There is an outgoing label corresponding to the FEC on the router that returns a Reply packet, indicating that the router that returns a Reply packet is an intermediate router of the LSP.
B	There is no outgoing label corresponding to the FEC on the router that returns a Reply packet, indicating that the LSP is interrupted.
D	Validation information carried in Downstream Mapping TLV does not match the information on the router that returns a Reply packet.
F	There is no FEC mapping carried in the corresponding TargetFec on the router that returns a Reply packet.

f	The label of the current label stack in the router that returns a Reply packet is inconsistent with the label of FEC mapping carried in TargetFec.
M	The format of the Request packet received by the router that returns a Reply packet is incorrect.
m	The Request packet received by the router that returns a Reply packet has TLVs that are not supported.
N	The router that returns a Reply packet does not have an instance corresponding to the incoming label, indicating that the labels are not synchronous.
P	The protocol for transmitting packets in the router that returns a Reply packet is inconsistent with that recorded in TargetFec stack.
p	Premature termination of packet transmission
R	Return the reserved value.
I	Upstream interface index unknown
X	Unknown return value
x	The return value is 0.

Related commands

Command	Description
traceroute mpls	View the LSRs that the MPLS LSP passes.

Platform description

None

1.1.45 propagate-release

Use this command to enable label release. Use the **no** form of this command to disable this function with no label release messages transmitted.

[**no**] **propagate-release**

Default configuration	Disabled
Command mode	**config-mpls-router** mode.
Usage guidelines	This command execution does not influence the label release messages previously received from the LDP instance, only the ones received later.

Examples	The following command enables label release of the LDP instance:
	`DES-7200(config)# mpls router ldp`
	`DES-7200(config-mpls-router)# propagate-release`

Related commands

Command	Description
show mpls ldp parameters	Show the LDP configuration parameters under all or specified VRFs.

1.1.46 snmp-server enable traps mpls

Use this command to enable Trap transmission of MPLS. Use the **no** form of this command to disable Trap transmission of MPLS.

snmp-server enable traps mpls {xc|ldp|vpn}
snmp-server enable traps mpls xc [xc-up] [xc-down]
snmp-server enable traps mpls ldp [pv-limit][session-down][session-up]
snmp-server enable traps mpls l3vpn [max-threshold] [mid-threshold][max-thresh-cleared][vrf-up][vrf-down]
no snmp-server enable traps mpls xc [xc-up] [xc-down]
no snmp-server enable traps mpls ldp [pv-limit][session-down][session-up]
no snmp-server enable traps mpls l3vpn [max-threshold] [mid-threshold][max-thresh-cleared][vrf-up][vrf-down]

Parameter description

Parameter	Description
xc	Trap transmmission switch for MPLS route

	change
ldp	Trap transmmission switch for LDP
l3vpn	Trap transmmission switch for L3 VPN
xc-up	Trap transmmission switch for MPLS route change XC Up
xc-down	Trap transmmission switch for MPLS route change XC Down
pv-limit	Trap transmmission switch for mismatch of path vectors
session-down	Trap transmmission switch for LDP sessions disconnected
session-up	Trap transmmission switch for LDP sessions created
max-threshold	Trap transmission switch for VRF maximum route threshold
mid-threshold	Trap transmission switch for VRF middle route threshold
max-thresh-cleared	Trap transmission switch for cleared VRF maximum route threshold
vrf-up	Trap transmmission switch for VRF Up
vrf-down	Trap transmmission switch for VRF Down

Default configuration	By default, traps of MPLS are sent.
Command mode	Global configuration mode

There are two types of XC traps:

1. XC Up trap, indicating that an effective ILM or FTN entry is generated
2. XC Down trap, indicating that an ILM or FTN entry is deleted

The user can enable the preceding two trap switches at the same time by using the **snmp-server enables mpls xc** command at the same time or either of them by using the **snmp server enables mpls xc [xc-up] [xc-down]** command.

There are three types of LDP traps:

1. LDP session Up trap, which is sent when an LDP session is established
2. LDP session Down trap, which is sent when an LDP session is disconnected
3. When initialization messages (INIT) are exchanged after an LDP session is established, a trap is sent if the value of the path vector list length used in loop detection does not match that advertised by the neighbor.

Usage guidelines

The user can enable the preceding three trap switches at the same time by using the **snmp-server enables mpls ldp** command or any of them by using the **snmp server enables mpls ldp [pv-limit] [sesseion-up] [session-down]** command.

There are the following types of L3 VPN traps:

1. Trap identifying VRF Up or Down: When an VRF instance has an associated interface Up, the VRF instance is considered to be in Up state. In this case, a VRF Up trap needs to be sent. When an VRF instance has all its associated interfaces Down or has no associated interface, a VRF Down trap needs to be sent.
2. Trap of VRF route pre-alert: When the number of VRF routes exceeds the middle route capacity threshold, a VRF MidThreshExceed trap is sent. When the number of VRF routes exceeds the maximum route capacity threshold, a VRF MaxThreshExceed trap is sent. In this case, a VRF MaxThreshCleared trap needs to be sent after the number of VRF routes becomes below the maximum route capacity threshold, indicating that the number of VRF routes returns to normal.

The user can enable all trap switches for L3 VPN at the same time by using the **snmp-server enables mpls l3vpn** command or any of them by using the **snmp server enables mpls l3vpn**

[max-threshhold] [mid-threshhold][max-thresh-cleared] [vrf-up] [vrf-down] command.

After MPLS Trap Transmission is enabled, to capture a trap on a host, you must use the **snmp-server host c**ommand to specify the host to receive the trap.

Examples

The following command configures Trap Transmission of LDP to be enabled:

DES-7200(config)#snmp-server host *192.168.10.1*

```
DES-7200(config)#snmp-server enable traps mpls ldp
```

Related commands

Command	Description
snmp-server host	Set a host for receiving traps.

Platform description

None

1.1.47 target-session holdtime

Use this command to set the keepalive holdtime for the extended mechanism. Use the **no** form of this command to restore the default value.

target-session holdtime *seconds*

Parameter description

Parameter	Description
seconds	Set the holdtime, with the value range *<15-65535>.*

Default configuration

By default, the holdtime of the LDP session built in the extended discovery mechanism is 180s. The sending interval of the keepalive message is 60s, which is 1/3 of the session holdtime.

Command mode	**config-mpls-router** mode.
Usage guidelines	Note that this command is valid for the LDP session only built in the extended discovery mechanism, not for the LDP session already set up.

Examples	The following command configures the keepalive holdtime for LDP sessions established by the extended mechanism:
	`DES-7200(config)#mpls router ldp`
	`DES-7200(config-mpls-router)# target-session holdtime 90`

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration parameters under all or specified.

1.1.48 traceroute mpls

Use this command to detect an MPLS LSP hop by hop and trace the LSRs that the LSP passes.

traceroute mpls ipv4 *ip-addressImask* [**timeout** *timeout*] [**ttl** *time-to-live*] [**source** *ip-address*] [**destination** *ip-address*] [**force-explicit-null**] [**reply mode** {**ipv4 | router-alert**}] [**flags fec**] [**verbose**]

Parameter description

Parameter	Description
ip-address/mask	IPv4 address and subnet mask length of the destination FEC to be tested
timeout *timeout*	(Optional) Specify the timeout time for packets, ranging from 0 to 3600, 2 by default
ttl *time-to-live*	(Optional) Specify the TTL value for sending packets, ranging from 1 to 255, 30 by default
source *ip-address*	(Optional) Source address. It is the destination address when the peer sends an Echo Reply packet.

	destination *ip-address*	(Optional) Specified 127/8 segment address. It is used to fill the IP header, 127.0.0.1 by default.
	force-explicit-null	(Optional) Whether to forcibly add an explicit null label to the MPLS label. By default, it is not added.
	reply mode {**ipv4** | **router-alert**}	(Optional) Specify the reply mode of the Echo Request packet: **ipv4**: reply with an IPv4 UDP packet (default) **router-alert**: reply with an IPv4 UDP packet with the Router Alert option
	flags fec	(Optional) Set forcible FEC stack check.
	verbose	(Optional) Show detailed information about Echo Reply packets. By default, the informaiton is not shown.

Default configuration	See the preceding parameter description.
Command mode	Privileged mode
Usage guidelines	You can change some default parameter values by specifying optional parameters. In addition to the directly typed command, interactive typing mode is provided. You can enter the interactive typing mode by pressing **Enter** after typing the **traceroute mpls** command.

Examples	To view the LSRs that the LSP of the FEC corresponding to 10.10.10.10/32 passes, type the following command:
	`DES-7200# traceroute mpls ipv4 10.10.10.10/32`
	`Tracing MPLS Label Switched Path to 10.10.10.10/32, timeout is 2 seconds`

```
      < press Ctrl+C to break >
Codes:'!' - success,'Q' - request not sent,'.'-timeout,
  'L'-labeled output interface,'B'-unlabeled output interface,
  'D'-DS Map mismatch,'F'-no FEC mapping,'f'-FEC mismatch,
  'M'-malformed request,'m'-unsupported tlvs,'N'-no label entry,
  'P'-no rx intf label prot,'p'-premature termination of LSP,
  'R'-transit router,'I'-unknown upstream index,
  'X'-unknown return code,'x'-return code 0
Type escape sequence to abort.
  0 10.3.0.8 MRU 1500 [Labels: 17 Exp: 0]
L 1 10.3.0.1 MRU 1504 [Labels: implicit-null Exp: 0] 624 ms
! 2 10.2.0.1 708 ms
```

See the **ping mpls** command for descriptions of return values.

Related commands

Command	Description
ping mpls	Detect the connectivity of an MPLS LSP.

Platform description

None

1.1.49 transport-address

Use this command to configure globally the transport address used by basic LDP sessions. Use the **no** form of this command to delete the configuration.

transport-address {interface | *ip-address* | *interface-name* }

no transport-address

Parameter description

Parameter	Description
interface	The primary IP address of an interface is used as the transport address for basic LDP sessions created on each interface.
Ip-address	The specified IP address is used as the

	transport address for all basic LDP sessions.
Interface-name	The primary IP address of the specified interface is used as the transport address for all basic LDP sessions.

Default configuration

Use the LSR ID of LDP as the transport address.

Command mode

config-mpls-router mode.

Usage guidelines

This command is ineffective to LDP sessions created by the extended discovery mechanism, and it is effective only to LDP sessions created by the basic discovery mechanism. LDP sessions created by the extended discovery mechanism always use the LSR ID of LDP as the transport address. If both an interface transport address and a global transport address are configured, the interface transport address have priority over the global transport address to take effect.

Examples

The following example configures the primary IP address of each interface as the transport address:

```
DES-7200(config)# mpls router ldp

DES-7200(config-mpls-router)# transport-address interface
```

Related commands

Command	Description
mpls ldp transport-address	Configure the transport address used by basic LDP sessions created on an interface.

Platform description

None

1.2 Showing Commands

1.2.1 show ip ref mpls forwarding-table

Use this command to show MPLS express forwarding information.

show ip ref mpls forwarding-table [**vrf** *vrf-name*] {**ftn** [*ip-address*/*mask*] | **ilm** [*label*]} [**frr**] [**detail**]

Parameter description

Parameter	Description
vrf *vrf-name*	Show the specified VRF entry information.
ftn [*ip-address/mask*]	Show FTN entry information.
ilm [*label*]	Show ILM entry information.
frr	Show FRR entry information when and only when there are active/standby FTN/ILM entries.
detail	Show detailed information about FTN/ILM entries.

Default configuration

None

Command mode

Privileged mode

Usage guidelines

Use this command to show MPLS express forwarding information as follows:

- If this command does not specify a VRF, it indicates that FTN/ILM entry information of all VRFs is displayed.

Examples

Example 1: To show FTN entry information of all VRFs, use the

following command:

```
DES-7200#show ip ref mpls forwarding-table ftn
Label Operation Code:
PH--PUSH label
IP--IP lookup forward
FEC      VRF  Out Label  OP  Out IF  Adj    Nexthop
1.1.1.1/32   0    1024    PH   2      7    20.0.0.6
2.2.2.2/32   0    1026    PH   4      3    21.1.1.1
```

FEC: In the case of FTN for IP routes, the IP address and mask are displayed for the FEC field; in the case of FTN for L3 VPN, "--" is displayed for the FEC field.

VRF: Indicates the VRF to which the FTN belongs.

Out Label: Indicates an outgoing label.

OP: Indicates an operation behavior that a packet hits the forwarding entry. This behavior includes the following:

Field	Description
PH	Indicates that an IP packet needs to be added with labels (perhaps one to three labels) and then forwarded to the next hop after hitting the entry. If imp-null is displayed for an outgoing label, the imp-null label is not added in the actual forwarding process.
IP	Indicates an IP packet needs to be forwarded across VRFs after hitting the entry. This type of entry is the forwarding entry across VRFs of one VPN.

Out IF: Indicates the outgoing interface for packet forwarding, using the interface index number.

Adj: Indicates adjacency identifier.

Nexthop: Indicates the next hop for packet forwarding. "--" is displayed for a forwarding entry with an ineffective next hop address.

Example 2: To show FRR information for FTN entries under all VRFs, use the following command:

```
DES-7200#show ip ref mpls forwarding-table ftn frr
Label Operation Code:
PH--PUSH label
IP--IP lookup forward
Status codes: m – main entry, b – backup entry, * – active
```

```
   FEC       VRF    Out Label  OP  Out IF  Adj    Nexthop
m*1.1.1.1/32   0     1024     PH  2      7     20.0.0.6
b 1.1.1.1/32   0     1025     PH  3      2     20.0.1.6
```

Example 3: To show ILM entry information of all VRFs, use the following command:

```
DES-7200#show ip ref mpls forwarding-table ilm
Label Operation Code:
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
PN--POP label and forward to nexthop
PI--POP label and do ip lookup forward
PC--POP label and continue lookup(IP or Label)
DP--DROP packet
```

PM--POP label and do MAC lookup forward

PV--POP label and output to VC attach interface

```
In Label    Out Label  OP  VRF   Out IF  Adj    Nexthop
1024        1028    SW  0       2     7    20.0.0.6
1025        1029    SW  0       3     2    20.0.1.6
```

In Label: Indicates an incoming label.

Out Label: Indicates an outgoing label.

OP: Indicates an operation behavior that a packet hits the forwarding entry. This behavior includes the following:

Field	Description
PP	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry, that is, perform forwarding of the last but one hop.
SW	Indicates that an MPLS packet needs to exchange labels and be forwarded to the next hop directly after hitting the entry.
SP	Indicates that an MPLS packet needs to exchange top labels, added with a label, and be forwarded to the next hop after hitting the entry. Exchanged labels are displayed for the outgoing label field, and one to two labels may be added.

PN	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry.
PI	Indicates that an MPLS packet needs to remove all labels and be forwarded according to the destination IP address after hitting the entry.
PC	Indicates that an MPLS packet removes the top label and is forwarded according to the query result in the label forwarding table after hitting the entry. In the case of an IP packet, it is forwarded according to the destination IP address.
PM	Indicates that an MPLS packet needs to remove the label and is forwarded according to the destination MAC of the inner packet (VPLS application) after hitting the entry.
PV	Indicates that an MPLS packet needs to remove the label and is forwarded from a specified egress (VPWS application) after hitting the entry.
DP	Indicates that a packet is discarded after hitting the entry.

VRF: Indicates the VRF to which the ILM belongs.

Out IF: Indicates the outgoing interface for packet forwarding, using the interface index number.

Adj: Indicates adjacency identifier.

Nexthop: Indicates the next hop for packet forwarding. "--" is displayed for a forwarding entry with an ineffective next hop address.

Example 4: To show FRR information for ILM entries under all VRFs, use the following command:

```
DES-7200#show ip ref mpls forwarding-table ilm frr
Label Operation Code:
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
PN--POP label and forward to nexthop
PI--POP label and do ip lookup forward
PC--POP label and continue lookup(IP or Label)
```

```
DP--DROP packet
Status codes: m – main entry, b – backup entry, * – active
  In Label    Out Label  OP  VRF    Out IF  Adj    Nexthop
m*1024        1028       SW  0       2      7     20.0.0.6
b 1024        1029       SW  0       3      2     20.0.1.6
```

Related commands

Command	Description
-	-

Platform description

None

1.2.2 show mpls forwarding-table

Use this command to show the MPLS forwarding table.

show mpls forwarding-table [*ip-address/mask*] [**label** *label*] [**interface** *interface-name*] [**next-hop** ***i****p-address*] [**ftn** [**ip** | **vc**]] [**ilm** [**ip** | **vc**]] [{**vrf** *vrf-name* | **global**} [**ftn** | **ilm**]] [**detail** | **summary**]

Parameter description

Parameter	Description
ip-address/mask	Show ILM and FTN entries of a specified FEC.
label *label*	Show the ILM entry of a specified label.
interface *interface-name*	Show the MPLS forwarding entry (ILM and FTN) of a specified egress.
next-hop *ip-address*	Show the MPLS forwarding entry (ILM and FTN) of a specified next-hop address.
ftn	Show an FEC mapping entry.
ilm	Show a label forwarding entry.
ip	Show the MPLS forwarding entry of an IP application (including unicast route and L3 VPN).

vc	Show the MPLS forwarding entry added by the vc.
vrf *vrf-name*	Show the MPLS forwarding entry related to a VRF.
detail	Show the detailed information about the MPLS forwarding entry.
global	Show global non-VRF MPLS forwarding entries, excluding FTN and ILM entries of VC.
summary	Show the statistics information of MPLS process forwarding.

Default configuration

No parameter is carried, indicating that all MPLS forwarding entries are displayed.

Command mode

Privileged mode

Usage guidelines

Use the **show mpls forwarding-table** command to show information about all MPLS forwarding entries (including ILM and FTN entries).

Use the **show mpls forwarding-table** *ip-address/mask* command to show information about specified MPLS forwarding entries (including ILM and FTN entries).

Use the **show mpls forwarding-table label** *label* command to show the ILM forwarding entries of a specified label.

Use the **show mpls forwarding-table interface** *interface-name* command to show the MPLS forwarding entries of a specified egress (including FTN and ILM entries).

Use the **show mpls forwarding-table next-hop** *ip-address* command to show the MPLS forwarding entries of a specified next hop (including FTN and ILM entries).

Use the **show mpls forwarding-table detail** command to show detailed information about all MPLS forwarding entries (including

ILM and FTN entries).

Use the **show mpls forwarding-table vrf** command to show all MPLS forwarding entries (including ILM and FTN entries) which belong to a VRF.

Use the **show mpls forwarding-table vrf** *vrf-name* **ftn** command to show information about all FTN entries which belong to a VRF.

Use the **show mpls forwarding-table vrf** *vrf-name* **ilm** command to show information about all ILM entries which belong to a VRF.

Use the **show mpls forwarding-table ftn ip** command to show FTN entries of unicast routes and L3 VPN application.

Use the **show mpls forwarding-table ilm ip** command to show ILM entries of unicast routes and L3 VPN application.

Use the **show mpls forwarding-table ftn** command to show all FTN entries.

Use the **show mpls forwarding-table ilm** command to show all ILM entries.

Use the **show mpls forwarding-table ftn vc** command to show all FTN entries of L2 VPN.

Use the **show mpls forwarding-table ilm vc** command to show all ILM entries of L2 VPN.

Use the **show mpls forwarding-table ftn detail** command to show detailed information about all FTN entries.

Use the **show mpls forwarding-table ilm detail** command to show detailed information about all ILM entries.

Examples

Example 1: To show all MPLS forwarding entries, to use the following command:

```
DES-7200#show mpls forwarding-table

Label Operation Code:

PH--PUSH label

PP--POP label

SW--SWAP label

SP—-SWAP topmost label and push new label

DP—-DROP packet

PC—-POP label and continue lookup by IP or Label

PI--POP label and do ip lookup forward
```

```
PN--POP label and forward to nexthop

PM--POP label and do MAC lookup forward

PV--POP label and output to VC attach interface

IP--IP lookup forward

Local Outgoing OP FEC        Outgoing      Nexthop

laebl label                   interface

--    1025      PH 119.1.1.0/24(V)  Gi3/19    10.0.10.1

--    1026      PH 120.1.1.0/24     Gi3/18      10.0.2.1

--    imp-null   PH 130.1.1.0/24    Gi3/18      10.0.2.1

1025  1027      SP 100.1.1.0/24     Vl8          192.1.2.1

1026  1028      SW 120.1.2.0/24     Gi3/19       10.0.2.1

1027  imp-null   PP 121.1.1.0/24    Fa3/1        11.0.0.1

--    --         IP 167.168.195.0/24 Fa3/2        120.1.1.1

1028  --         PC 167.168.196.0/24 --           --

1029  --         PN 167.168.197.0/24(V) Vl4       1.0.0.1

1030  --         PI VRF(vpna)         --          --

1031  --         PV VC(20,1.1.1.1)    Vl5          --

--    1029       PH VC(20,1.1.1.1)    Vl10         192.1.2.1

1032  --         PI 192.1.1.0/24(V)  Vl101        172.2.1.2

1033  1030       SW 193.1.1.0/24(V)  Vl102        10.2.1.2
```

Local label: It is the label distributed by this forwarding equivalence class device to other devices, namely the incoming label of an ILM entry. If there is no incoming label for an FTN entry, "--" is displayed.

Outgoing label: It is the outgoing label of an ILM or FTN label. "--" indicates that an ILM or FTN label has no outgoing label. If impl-null is shown, it indicates an implicit null label 3 and that this label is not carried in the forwarding of packets.

OP: Indicates an operation behavior that a packet hits the incoming label and outgoing label of a forwarding entry (ILM or FTN), and the behavior includes the following:

Field	Description

PH	Indicates that an IP packet needs to be added with labels (perhaps one to three labels) and then forwarded to the next hop after hitting the entry. Use the **show mpls forwarding-table detail** command to view the labels and the number of labels added. If imp-null is displayed for an outgoing label, the imp-null label is not added in the actual forwarding process.
PP	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry, that is, perform forwarding of the last but one hop.
SW	Indicates that an MPLS packet needs to exchange labels and be forwarded to the next hop directly after hitting the entry.
SP	Indicates that an MPLS packet needs to exchange top labels, added with a label, and be forwarded to the next hop after hitting the entry. Exchanged labels are displayed for the outgoing label field. Use the **show mpls forwarding-table detail** command to the labels added and the number of labels. One to two labels may be added.
PN	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry.
PI	Indicates that an MPLS packet needs to remove all labels and be forwarded according to the destination IP address after hitting the entry.
PC	Indicates that an MPLS packet removes the top label and is forwarded according to the query result in the label forwarding table after hitting the entry. In the case of an IP packet, it is forwarded according to the destination IP address.
PM	Indicates that an MPLS packet needs to remove the label and is forwarded

	according to the destination MAC of the inner packet (VPLS application) after hitting the entry.
PV	Indicates that an MPLS packet needs to remove the label and is forwarded from a specified egress (VPWS application) after hitting the entry.
IP	Indicates an MPLS packet needs to be forwarded across VRFs after hitting the entry. This type of entry is the forwarding entry across VRFs of one VPN.
DP	Indicates that a packet is discarded after hitting the entry.

FEC: It has two meanings.

1. In the case of an FTN entry ("--" is displayed if it has no incoming label), the IP address and mask are displayed for the FEC field if the FTN is for IP route. If (V) is carried behind, it indicates that the FTN belongs to a VRF. In the case of a VC FTN, VC ID and VC peer IP are displayed for the FEC field.

2. For an ILM entry (it has an incoming label), if the label is for IP route, the IP address and mask are displayed for the FEC field. If (V) is carried behind, it indicates that the ILM belongs to a VRF. If the label is for a VRF of an L3 VPN (that is, each VRF of a VPN is allocated with a label), the VRF name is displayed for the FEC field, such as VRF (vpna) in the preceding example. If the label is for VC, VC ID and VC peer IP are displayed for the FEC field, such as VC (20,1.1.1.1) in the preceding example.

Outgoing interface: Indicates the outgoing interface for packet forwarding and uses the abbreviated name of the interface.

Nexthop: Indicates the next hop for packet forwarding. "--" is displayed for a forwarding entry with an ineffective next hop address.

Example 2: The following command shows statistics information of the process forwarding module:

```
DES-7200# show mpls forwarding-table summary

MPLS forwarding is ON

Enable count:1

ILM entrys:14

ILM changes:14
```

```
ILM failed changes :0

IP FTN entrys:0

IP FTN changes:4

IP FTN failed changes:0

L2 FTN entrys:0

L2 FTN changes:0

L2 FTN failed changes:0

In label packets:0

Out label packets:0

Send label packets:0

In ip packets:0

Out ip packets:0

Out ip stack packets:0

Forwarding packets:0

Fragment packets:0

Fragment error packets:0

Label error packets:0

Label failed packets:0

Ttl over packets:0

Buffer failed packets:0

Ip don't fragment packets:0

Other failed packets:0
```

Example 3: The following command shows FRR information of the process forwarding module:

```
DES-7200#show mpls forwarding-table frr

Label Operation Code:

PH--PUSH label

PP--POP label
```

```
SW--SWAP label

SP--SWAP topmost label and push new label

DP--DROP packet

PC--POP label and continue lookup by IP or Label

PI--POP label and do ip lookup forward

PN--POP label and forward to nexthop

PM--POP label and do MAC lookup forward

PV--POP label and output to VC attach interface

IP--IP lookup forward

Status codes: m – main entry, b – backup entry, * – active.

   Local  Outgoing   OP  FEC             Outgoing    Nexthop

   Label  label                        interface

m* --    1026      PH  120.1.1.0/24     Gi3/18      10.0.2.1

b  --    1027      PH  120.1.1.0/24     Gi3/19      10.0.3.1

m* 1028   1029      SW  120.1.2.0/24     Gi3/18      10.0.2.1

b  1028   1030      SW  120.1.2.0/24     Gi3/29      10.0.3.1
```

1.2.3 show mpls label-pool

Use this command to show the usage of the label pool in various label spaces. You can show the data of all the label spaces, or that of a specific label space by specifying a label space number.

show mpls label-pool [*label_space*]

Parameter description

Parameter	Description
label_space	Specify the label space whose label pool is to be shown.

Default configuration

None

Command mode	Privileged mode
Usage guidelines	This command allows you to show the usage of the label pools of all label spaces or a specific label space, including label pool size, maximum/minimum label value, and allocation of each label pool. At present, only the global label space is supported.

Examples

```
DES-7200# show mpls label-pool
label space: 0
label pool bucket size 512
min label 16, max label 1048575
label block used 2, free 2046
status codes: (s) – stale
CLI: 0   , 1    (Include label [16,1023], reserved)
LDP: 3   , 4 (s)
```

Related commands

Command	Description
label-switching	Enable label switching.

1.2.4 show mpls ldp bindings

Use this command to show the LDP label binding information, which can be filtered according to VRF, FEC prefix, label value, remote binding, or local binding.

show mpls ldp bindings [**all** | **vrf** *vrf-name*] [*ip-address* **|** *mask* | **label** *label*] [**remote** | **local**]

Parameter description

Parameter	Description
all	Show label binding information under all VRFs.
vrf *vrf-name*	Show label binding information under specified VRFs.
ip-address | *mask*	Show label binding information of specified FECs.

label *label*	Show label binding information of specified label values, ranging from 0 to 1048575.
remote	Show remote label binding information received from the LDP peer.
local	Show label binding information sent locally.

Default configuration

No parameter is carried, indicating that all label binding information under the global VRF is shown.

Command mode

Privileged mode

Usage guidelines

This command shows the FEC and label binding information. This command allows you to view the working status of the LDP, whether the LDP has normally bound a label to an FEC, the specific label value of bound to an FEC, and whether the binding is local binding or remote binding. If no VRF is specified, it indicates that label binding information under the global VRF is displayed.

Examples

The following command shows label database informaiton under the global VRF:

```
DES-7200# show mpls ldp bindings
Default VRF:
  lib entry: 2.2.2.2/32
     local binding:  to lsr:10.20.10.10:0,label: imp-null
     remote binding: from lsr:10.20.10.10:0,label: 16 (not in FIB)
  lib entry: 10.20.10.10/32
     local binding:  to lsr:  10.20.10.10:0, label: 1027
     remote binding: from lsr: 10.20.10.10:0, label: imp-null
```

Field	Description
local binding	Label binding information distributed by an LSR

	for an FEC. not in FIB indicates that the information is not added to the FIB.
remote binding	Remote label binding information received from the LDP peer. not in FIB indicates that the information is not added to the FIB.

Related commands

Command	Description
show mpls ldp neighbor	Show the LDP session status.

1.2.5 show mpls ldp discovery

Use this command to show the neighbor information discovered by LDP under all or specified VRFs.

show mpls ldp discovery [**all** | **vrf** *vrf-name*] [**detail**]

Parameter description

Parameter	Description
all	Show the neighbor information discovered by LDP under all VRFs.
vrf *vrf-name*	Show the neighbor information discovered by LDP under specified VRFs.
detail	Show detailed information about neighbors discovered by LDP.

Default configuration

None

Command mode

Privileged mode

Usage guidelines

This command allows you to show the interfaces on which LDP neighbors have been discovered, the LDP neighbors discovered, the Hello packet source address of the LDP neighbor, and Hello keepalive time. Specifying no VRF indicates that neighbor information discovered by LDP under the global VRF is displayed.

Examples

The following command shows neighbor information discovered by LDP under the global VRF:

```
DES-7200# show mpls ldp discovery
Default VRF:
 Local LDP Identifier:
    8.8.8.8:0
    Discovery Sources:
    Interfaces:
       GigabitEthernet 2/1 (ldp): xmit/recv
          LDP Ident: 10.30.10.10:0
       GigabitEthernet 2/2 (ldp): xmit
    Targeted Hellos:
       8.8.8.8 -> 10.5.0.1 (ldp): active, xmit
       8.8.8.8 -> 10.30.10.10 (ldp): active/passive, xmit
       2.2.2.2 -> 10.30.10.10 (ldp): passive, xmit/recv
             LDP Ident: 10.30.10.10:0
```

Field	Description
Local LDP Identifier	Indicates the LDP identifier for the local router.
Interfaces	Indicates the interface information lists discovered by the active LDP.
xmit	Indicates that Hello packets were sent on an interface.
recv	Indicates that Hello packets are received on an interface.
Targeted Hellos	Indicates the sending path list of all targeted Hello messages.
active	Indicates the local LSR actively sends targeted Hello messages.

	passive	Indicates the neighbor LSR actively sends targeted Hello messages. The local LSR is configured to respond to the targeted Hello message sent by the neighbor LSR.

	Command	Description
Related commands	**show mpls ldp interface**	Show the LDP-enabled interface information.
	neighbor *ip-address*	Create an LDP extended peer.

1.2.6 show mpls ldp graceful-restart

Use this command to show the LDP GR session and its parameters.

show mpls ldp graceful-restart [**all** | **vrf** *vrf-name*]

	Parameter	Description
Parameter description	**all**	Show LDP GR sessions and session parameters of all VRFs (inlcuding VRF).
	vrf *vrf-name*	Show LDP GR sessions and session parameters of specified VRFs.

Default configuration	None

Command mode	Privileged mode

Usage guidelines

Use this command to show the LDP GR session and session parameter as follows:

- If there is no parameter in this command, it indicates that the LDP GR sessions and session parameters of the global VRF are displayed.

Examples

The following command shows the LDP GR sessions and session parameters:

```
DES-7200# show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (1 records):
    Peer LDP Ident: 20.20.20.20:0; Local LDP Ident: 10.10.10.10:0
        Status: recovering (86 seconds left)
        Address list contains 3 addresses:
          192.168.202.3   20.20.20.20    192.168.201.37
  Graceful Restart-enabled Sessions:
    Peer LDP Ident: 20.20.20.20:0, State: estab
```

Field	Description
Default VRF	Global VRF information
LDP Graceful Restart is enabled	The GR capability of LDP is enabled for a VRF.
Neighbor Liveness Timer	Survival time of the neighbor timer in the unit of second
Max Recovery Time	Maximum recovery time in the unit of second
Forwarding State Holding Time	Forwarding state holding time (reconnect time) in the unit of second
Down Neighbor Database	Down database information of an LDP neighbor
Graceful Restart-enabled Sessions	Enable LDP session information of LDP GR.
Peer LDP Ident	Peer LDP ID
State	LDP session state of an LDP

	neighbor

	Command	Description
Related commands	**graceful-restart**	Enable the GR capability of LDP.
	graceful-restart timer reconnect *seconds*	Configure the reconnect time of an LDP session.
	graceful-restart timer neighbor-liveness *seconds*	Configure the survival time of an LDP neighbor.
	graceful-restart timer recovery *seconds*	Configure the recovery time of an LDP session.

1.2.7 show mpls ldp interface

Use this command to show information about interfaces enabled with LDP under all or specific VRFs.

show mpls ldp interface [**all** | **vrf** *vrf-name* | *interface-name*]

	Parameter	Description
Parameter description	**all**	Show information about interfaces enabled with LDP under all VRFs.
	vrf *vrf-name*	Show information about interfaces enabled with LDP under specified VRFs.
	interface-name	Show information about specified interfaces.

Default configuration	None

Command mode	Privileged mode
Usage guidelines	Use this command to show the device's interfaces on which LDP is enabled and Up/Down state of them. If no VRF is specified, it indicates that interface information under the global VRF is displayed.

Examples

The following command shows information about the interfaces enabled with LDP under the global VRF:

```
DES-7200# show mpls ldp interface
Default VRF:
Interface              Operational    Status
GigabitEthernet 2/1    Yes            UP
GigabitEthernet 2/2    No             DOWN
GigabitEthernet 2/3    Yes            UP
```

Field	Description
Operational	Indicates whether an interface is enabled with LDP.
Status	Indicates interface status.

1.2.8 show mpls ldp neighbor

Use this command to show LDP neighbor information under all or specified VRFs.

show mpls ldp neighbor [**all** | **vrf** *vrf-name*] [*ip-address*] [**detail**]

Parameter description

Parameter	Description
all	Show LDP session information under all VRFs.
vrf *vrf-name*	Show LDP session information under specified VRFs.
ip-address	Show LDP session information of specified LDP peers under specified or all VRFs.
detail	Show detailed LDP session information.

Default configuration	None
Command mode	Privileged mode
Usage guidelines	Use this command to show all LDP neighbors, such as the TCP connection port between the local LDP and peer LDP, LDP status, received/sent message counts.

Examples

The following command shows LDP neighbor information under the global VRF:

```
DES-7200# show mpls ldp neighbor
Default VRF:
 Peer LDP Ident: 10.20.10.10:0; Local LDP Ident: 8.8.8.8:0
    TCP connection: 10.20.10.10.62488 - 8.8.8.8.646
    State: OPERATIONAL; Msgs sent/recv: 42/45; UNSOLICITED
    Up time: 00:33:49
    Graceful Restart enabled; Peer reconnect time (msecs): 300000
  Down Neighbor Information:
    Status: recovering (115 seconds left)
    LDP discovery sources:
 Link Peer on GigabitEthernet 2/1,Src IP addr:192.168.201.220
    Targeted Hello 8.8.8.8 -> 10.20.10.10
    Addresses bound to peer LDP Ident:
      10.20.10.10   192.168.201.220 192.168.198.1   10.5.0.1
```

Field	Description
Peer LDP Ident	Peer LDP identifier of an LDP session
Local LDP Identifier	LDP identifier of the local router
TCP connection	TCP connection that supports the LDP session
State	LDP session state

Msgs sent/recv	Count of LDP messages which are sent to and received from the session peer
UNSOLICITED&ONDEMAND	Label distribution mode
Up time	Time when an LDP session is established
Graceful Restart enabled	Indicates that Graceful Restart is enabled.
Peer reconnect time (msecs)	Reconnect time of the peer LDP session
Down Neighbor Information	Neighbor Down information
Status	Indicates that the neighbor is recovering (with 115 seconds to go).

Related commands

Command	Description
show mpls ldp discovery	Show the neighbor information discovered by LDP.

1.2.9 show mpls ldp parameters

Use this command to show the LDP configuration parameters under all or specified VRFs.

show mpls ldp parameter [**all** | **vrf** *vrf-name*]

Parameter description

Parameter	Description
all	Show LDP configuration parameters under all VRFs.
vrf *vrf-name*	Show LDP configuration parameters under specified VRFs.

Default configuration

None

Command mode

Privileged mode

Usage guidelines

Use this command to show various attribute information of LDP, including the LSR ID, transport address, loop detection mechanism, label distribution and control mode, label retention mode, interval and holdtime of the Hello packet for the extended mechanism as well as the interval and holdtime of the Keepalive packet. If no VRF is specified, it indicates that configuration parameters of LDP under the global VRF are displayed.

Examples

The following command shows the configuration parameters of LDP under the global VRF:

```
DES-7200# show mpls ldp parameters
Default VRF:
  Protocol version: 1
    Ldp Router ID: 1.1.1.1
    Control Mode: INDEPENDENT
    Propogate Release: FALSE
    Label Merge: TRUE
    Label Retention Mode: LIBERAL
    Loop Detection Mode: off
    Targeted Session Keepalive HoldTime/Interval: 180/60 sec
    Targeted Hello HoldTime/Interval: 45/5 sec
    LDP initial/maximum backoff: 15/120 sec
```

Related commands

Command	Description
ldp router-id	Configure the LDP router ID.
ldp-control-mode	Configure the LDP control mode.
ldp-label-retention -mode	Configure the label retention mode.
propagate-release	Configure the label propagate release switch.
label-merge	Configure the label merge switch.

	loop-detection-mode	Configure loop detection.

1.2.10 show mpls rib

Use this command to show MPLS RIB information.

show mpls rib [**all** | **vrf** *vrf-name*]

Parameter description

Parameter	Description
all	Show MPLS routing information under all VRFs.
vrf *vrf-name*	Show MPLS routing information under specified VRFs.

Default configuration

None

Command mode

Privileged mode

Usage guidelines

Use this command to show MPLS routing information as follows:

- If no parameter is specified in this command, it indicates that MPLS routing information under the global VRF is displayed.

Examples

The following command shows MPLS routing information under the global VRF:

```
DES-7200#show mpls rib
Status codes: m – main entry, b – backup entry, * – active, s – stale.
Default VRF:
  LSP Information    Total
  STATIC LSP         0
  LDP LSP            3
```

```
  RSVP LSP          0

  BGP LSP           0

  L3VPN LSP         0

LDP LSP:

  ------------------------------------------------------------------

   FEC            In/Out Label    In/Out IF      Nexthop

   119.1.1.0/24    -/1025          -/Gi3/19       10.0.10.1

   m* 120.1.1.0/24    -/1026          -/Gi3/18       10.0.2.1

   b  120.1.1.0/24    -/1031          -/Gi3/19       10.0.10.1

   m* 120.1.2.0/24    1027/1032       Gi3/10/Gi3/18   10.0.2.1

   b  120.1.2.0/24    1027/1033       Gi3/10/Gi3/19   10.0.10.1

------------------------------------------------------------------
```

Field	Description
LSP Information	● STATIC LSP: This type of LSP is configured manually. ● LDP LSP: This type of LSP is established through LDP. ● RSVP LSP: This type of LSP is an MPLS TE tunnel established through RSVP-TE. ● BGP LSP: This type of LSP is established through BGP for IPv4 private network BGP routes or IPv4 public network BGP routes. ● L3VPN LSP: This type of LSP is established through BGP for received VPNv4 routes.
Total	Show the total amount of LSP information related to a VRF.
FEC	Its value is usually the destination address of an LSP.
In/Out Label	Value of the incoming/outgoing label
In/Out IF	Name of the incoming/outgoing interface
Nexthop	Next hop

Related commands

Command	Description
-	-

Platform description

None

1.2.11 show mpls summary

Use this command to show MPLS global configuration information.

show mpls summary

Parameter description

Parameter	Description
-	-

Default configuration

None

Command mode

Privileged mode

Usage guidelines

This command allows you to view the basic information about MPLS, including maximum/minimum available labels, information about each label space, label space used by each interface, and total number of interfaces with MPLS enabled.

Examples

DES-7200# show mpls summary

`Per label-space information:`//Show information about each label space, with only label space 0 supported at present.

`Label-space 0 is using minimum label:16 and maximum label:1048575`//Label scope allowed by this label space

`Label-switching Interface:`//Display the interface enabled with label switching

Interface	Label space
GigabitEthernet 4/1	0
GigabitEthernet 4/2	0

```
Total number of mpls interface is 2
```

Related commands

Command	Description
label-switching	Enable label switching.

2 BGP/MPLS L3 VPN Configuration Commands

2.1 Configuration Related Commandss

2.1.1 address-family(VRF)

Use this command to configure the IPv4 or IPv6 address family for the multi-protocol VRF.

address-family {ipv4 | ipv6}

Parameter description

Parameter	Description
-	-

Default configuration

No IPv4 or IPv6 address family is configured for the multi-protocol VRF.

Command mode

VRF configuration mode

Usage guidelines

Configuring the IPv4 address family for the multi-protocol VRF is equivalent to enabling the IPv4 protocol. Configuring the IPv6 address family for the multi-protocol VRF is equivalent to enabling the IPv6 protocol.

Examples

Define the multi-protocol VRF vrf1, and configure the IPv4 address family.

```
DES-7200(config)#vrf definition vrf1
DES-7200(config-vrf)#address-family ipv4
DES-7200(config-vrf-af)#
```

Related commands

Command	Description
exit-address-family	Exit the configuration mode for the VRF address family.
vrf definition	Define the multi-protocol VRF.

2.1.2 address-family ipv4 vrf (BGP)

Use this command to enter or exit from the VRF address family mode, and set the interaction of a vrf route.

[no] address-family ipv4 vrf *vrf-name*

Parameter description

Parameter	Description
vrf-name	VRF name.

Default configuration

By default, no VRF address family is defined.

Command mode

Router configuration mode.

Usage guidelines

This command allows you to enable (or disable) the routing information exchange between the PE and CE. Use command **exit-address-family** to return to the BGP configuration mode.

Examples

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# address-family ipv4 vrf vrf1
```

Related commands

Command	Description
neighbor activate	Activate an address family.

	exit-address-family	Exit from this mode.

2.1.3 address-family vpnv4 (BGP)

Use this command to enter or exit from the VPN address family mode and enable VPN routing information interaction between the PEs.

[**no**] **address-family vpnv4** [**unicast**]

Parameter description

Parameter	Description
unicast	Specify the unicast address prefix

Default configuration

By default, no vpn address family is defined.

Command mode

Router mode

Usage guidelines

Use this command to enable the VPN routing information interaction between PEs and enter the **address-family VPN** mode. Use command **exit-address-family** to exit from the **address-family VPN** configuration mode.

Examples

```
DES-7200(config)# router bgp 100
DES-7200 (config-router)# address-family vpnv4
```

Related commands

Command	Description
neighbor activate	Activate an address family
exit-address-family	Exit from this mode.

2.1.4 alloc-label

Use this command to allocate label per VPN.

[**no**] **alloc-label** {**per-vrf** | **per-route**}

Parameter description

Parameter	Description
per-vrf	Allocate a label per VPN.
per-route	Allocate a label per VPN route.

Default configuration

By default, a label is allocated per VRF.

Command mode

VRF configuration mode

Usage guidelines

RFC4364 outlines two lable assignment methods for L3VPN: per route and per VRF. The former method rapidly forwards packets to the next hop by label by searching the ILM table, but it requires a large ILM table. For the latter method, all routes of a VRF share the label that significantly reduces the size of the ILM table, but its forwarding efficiency is lower for it searches the ILM table two times. First it searches the VRF of a packet from the ILM table, then forwards the packet according to the destination IP address of the routing table of the VRF.

Examples

To configure label assignment per route for VPNA, use the following command:

```
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# alloc-label per-route
```

2.1.5 area sham-link

Use this command to configure a sham link, and the **no** command is used to delete the corresponding sham link.

area *area-id* **sham-link** *source-address destination-address* [**cost** *number*] [**dead-interval** *seconds*] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**authentication** [**message-digest | null**]] [[**authentication-key** *key*] **|** [**message-digest-key** *key-id* **md5** *key*]]

no area *area-id* **sham-link** *source-address destination-address* [**cost**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**authentication**] **[**[**authentication-key**] **|** [**message-digest-key** *key-id*]]

Parameter description

Parameter	Description
area-id	It indicates the OSPF area ID of the sham link that can be a decimal integer ranging from 0 to 4294967295 or an IP address.
source-address	Sham link source address
destination-address	Sham link destination address
cost *number*	(Optional) It indicates the COST value for OSPF to send packets on the sham link. It ranges from 0 to 65535 with the default value of 1.
dead-interval *seconds*	(Optional) It indicates the time interval when the neighbor of the sham link dies. It ranges from 0 to 2147483647 with the default value of 40s.
hello-interval *seconds*	(Optional) It indicates the time interval for sending the Hello packet on the sham link. It ranges from 1 to 65535 with the default value of 10s.
retransmit-interval *seconds*	(Optional) It indicates the retransmission time interval for sending packets on the sham link. It ranges from 0 to 65535 with the default value of 5s.
transmit-delay *seconds*	(Optional) It indicates the delay for transmitting the LSU packet on the sham link. It ranges from 0 to 65535 with the default value of 1s.
authentication-key *key*	(Optional) It defines the key for OSPF plain text authentication. The keys for plain text authentication between neighbors must be consistent. The **service password-encryption** command can make the key to be displayed in an encrypted way.

message-digest-key *key-id* **md5** key	(Optional) It defines the key identifier and key for OSPF MD5 authentication. The key identifier and key for MD5 authentication between neighbors must be consistent. The **service password-encryption** command can make the key to be displayed in an encrypted way.
authentication	Set the authentication type: plain text authentication.
message-digest	Set the authentication type to MD5 authentication.
null	Set authentication not to be carried out.

Default configuration

By default, authentication is not carried out.

Command mode

OSPF Router mode

Usage guidelines

This command is valid only to the OSPF instance that associates the VRF.

To configure a sham link, configure the two PEs that set up the sham link. If you configure only one PE, the sham link cannot be set up.

The two PEs that establish the sham link must meet the following configuration requirements:

The sham link area-id of two PEs must be the same.

The source address of the sham link configured on one PE must be equal to the destination address of the sham link configured on the other PE.

The source address of the sham link configured on the PE must be a 32-bit loopback address, and this address must be bound to the corresponding VRF instance.

As the OSPF route announced through the sham link lacks a VPN tag, this route cannot be used for forwarding, and the actual forwarding still needs to use the BGP VPNv4 route. Therefore, during the actual configuration, the route announced through the sham link must announce the VPNv4 route to the related BGP neighbor through the MP-BGP protocol.

	 **Caution** The source address for setting up a sham link must participate in the BGP VPNv4 route announcement, but cannot participate in the calculation of the VRF OSPF instance.

Examples

A sham link is configured for an OSPF instance. The sham link belongs to the area 0, the source address is 1.1.1.1, the destination address is 2.2.2.2, and the COST value for transmitting packets on the sham link by the OSPF protocol is 10.

```
DES-7200(config)# router ospf 10 vrf vpn1
DES-7200(config-router)# area 0 sham-link 1.1.1.1 2.2.2.2 cost 10
```

Related commands

Command	Description
show ip ospf sham-links	Show all sham-link information of the OSPF instance.

Platform description None

2.1.6 bgp default route-target filter

Use this command to enter the automatic router-target filtering of BGP. Use the **no** form of this command to disable this function.

bgp default route-target filter

no bgp default route-target filter

Default configuration Enabled

Command mode BGP configuration mode

Usage guidelines

By default, a PE will refues the VPN route from other PE or ASBR which is not imported by any VRF on it. Using the **no** form of this command allows a PE to receive all VPN routes from other PEs or ASBR, no matter whether the VRFs on it imports the VPN routes or not.

This command is used for inter-domain VPN OptionB solution. Since no VRF is configured on an ASBR, but the ASBR needs to save VPN routes and advertise them to other PE (or ASBR), you need to run the **no bgp default route-target filter** command.

Caution

After the BGP peers are established and VPN routes are distributed, changing this configuration takes no effect for received or refused VPN routes. So it is recommended to use the **clear ip bgp** command to reset the sessions with the BGP peers, exchange VPN routes and determine whether to receive VPN routes.

For example, you run the **bgp default route-target filter** command to automatically filter route-target attribute. After the BGP peers are established and VPN routes are distributed, you need to disable this function. Hence, run the **no bgp default route-target filter** command and then the **clear ip bgp** command to reset the sessions with the BGP peers.

Examples

```
DES-7200(config)# router bgp 100
DES-7200 (config-router)# no bgy default route-target filter
```

2.1.7 capability vrf-lite

Use this command to control the loop inspection of the OSPF instance, and the no command enables loop inspection.

capability vrf-lite

no capability vrf-lite

Parameter description

Parameter	Description
-	-

Default

By default, the OSPF instance associated with the VRF supports loop

configuration	inspection.

Command mode	OSPF Router mode

Usage guidelines

This command is valid only for the OSPF instance associated with the VRF.

By default, the OSPF instance associated with the VRF supports loop inspection and the PE-CE OSPF feature (the so-called PE-CE OSPF feature is to convert different OSPF LSAs to CE based on the BGP extension attribute). Configuring the **capability vrf-lite** command will disable the function above. Loop inspection of the OSPF instance is to prevent the possible loop during transmission through the VPN route. The OSPF instance associated with the VRF will deal with the received LSAs according to the following rules:

LSA Type	Implementation Process
Types 3, 5, 7 LSA	Inspect the DN bit. If the received LSA has a DN bit, the LSA will not participate in the OSPF calculation.
Types 5, 7 LSA	Inspect the VPN domain-tag. If the VPN domain-tag of the received LSA and the VPN domain-tag of the local OSPF instance are the same, the LSA will not participate in the OSPF calculation.

After receiving the LSA packet, the OSPF protocol will not inspect the DN bit and the VPN domain-tag in the LSA packet, and let the LSA participate in the OSPF calculation. Disabling the PE-CE OSPF feature (for the introduction to “PE-CE OSPF Feature”, please see the *MPLS Configuration Guide*) means that different OSPF LSAs are not converted based on the BGP attribute.

By default, the OSPF instance associated with the VRF supports loop inspection.

The purpose of loop inspection is expected to disable the loop inspection of the VRF OSPF instance in some scenarios. For example, assume that a VPN user uses an MCE device exchange VPN routes with a PE. If the OSPF protocol runs for VPN route exchange between the MCE and PE and the MCE and VPN site exchange VPN routes through the EBGP, the OSPF and BGP in the MCE should be set to redistribute each other. To enable the BGP to completely redistribute OSPF routes, it is required to disable loop inspection of the VRF OSPF instance in the MCE by using the **capability vrf-lite** command.

Examples

Disable loop inspection of the OSPF instance.

```
DES-7200(config)# router ospf 10 vrf vpn1
DES-7200(config-router)# capability vrf-lite
```

Related commands

Command	Description
domain-tag	Configure domain-tag information of the OSPF instance.

Platform description

None

2.1.8 clear ip bgp vrf

Use this command to reset the sessions of all members in VRF.

clear ip bgp vrf *vrf-name* [*| *address*] [[**soft**][**in|out**]]

Parameter description

Parameter	Description
vrf-name	VRF name.
*	Reset all BGP sessions in VRF.
address	Reset the BGP sessions of the specified peer in VRF.
ipv4 unicast	IPv4 unicast session.
in	Reset the actively-connected session bulit by the peer.
out	Reset the actively-connected session bulit by the local BGP speaker.
soft	Reset the route information sent to or received from the specified peer by command.
soft in	Reset the received route information by command.

	soft out	Reset the distributed route information by command.

Default configuration	N/A.
Command mode	Privileged EXEC mode
Usage guidelines	Use this command to reset the BGP sessions of all members in VRF.
Examples	`DES-7200(config)# clear ip bgp vrf my-vrf in`

2.1.9 description

Use this command to set the VRF descriptor.

description *string*

Parameter description

Parameter	Description
string	Character string containing a maximum of 244 characters

Default configuration	None
Command mode	VRF configuration mode
Usage guidelines	None

Examples

Example 1: Define a single-protocol IPv4 VRF vrf1 and set the descriptor to vpn-a.

```
DES-7200(config)#ip vrf definition vrf1
DES-7200(config-vrf)#description vpn-a
```

Example 2: Define a multi-protocol VRF vrf2 and set the descriptor to vpn-b.

```
DES-7200(config)#vrf definition vrf1
DES-7200(config-vrf)#description vpn-b
```

Related commands

Command	Description
ip vrf	Define a single-protocol IPv4 VRF.
vrf definition	Define a multi-protocol VRF.

2.1.10 exit-address-family (BGP)

Use this command to exit the VRF family address configuration or VPN family address configuration mode.

exit-address-family

Parameter description

Parameter	Description
-	-

Default configuration

None

Command mode

Specific address family configuration mode

Usage guidelines

None

Examples

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# exit-address-family
```

Related

Command	Description

commands	-	-

Platform description None

Command history	**Version No.**	**Description**
	-	-

2.1.11 exit-address-family(VRF)

Use this command to exit the VRF address family configuration mode.

exit-address-family

Parameter description	**Parameter**	**Description**
	-	-

Default configuration None

Command mode VRF address family configuration mode

Usage guidelines None

Examples

Create a multi-protocol VRF vrf1 and configure an IPv4 address family.

```
DES-7200(config)#vrf definition vrf1
DES-7200(config-vrf)#address-family ipv4
DES-7200(config-vrf-af)# exit-address-family
DES-7200(config-vrf)#
```

Related commands	**Command**	**Description**
	address-family	Configure an IPv4 or IPv6 address family for a multi-protocol VRF.

	vrf definition	Define a multi-protocol VRF.

2.1.12 domain-id

Use this command to configure the domain ID of the OSPF instance. The no command is used to cancel the domain ID of the OSPF instance.

domain-id {*ip-address* [secondary] | null | type {0005|0105|0205|8005} value *hex-value* [secondary]}
no domain-id [*ip-address* [secondary] | null | type {0005|0105|0205|8005} value *hex-value* [secondary]]

Parameter description

Parameter	Description
ip-address	Set the domain ID to the IP address.
secondary	The configured domain ID serves as the secondary identifier.
null	The OSPF instance has no domain ID.
type {0005|0105|0205|8005}	Set the domain ID type of the OSPF instance. It has the following four values: 0x0005, 0x0105, 0x0205, 0x8005, and the default type is 0x0005.
value *hex-value*	Set the domain ID of the OSPF instance which is a hexadecimal numeral containing six bytes.
secondary	The configured domain ID serves as the secondary identifier.

Default configuration

By default, the domain-id value of the OSPF instance is NULL, and the type is 0005.

Command mode

OSPF Router mode

Usage guidelines

This command is valid only for the OSPF instance associated with the VRF.

Assume that the OSPF instance is configured with a domain ID. When an OSPF route changes into a VPN route after redistributed to BGP, the domain ID is also redistributed to the BGP, and is finally announced to other PEs as a part of the extended community attribute of the VPN route.

The OSPF instance can be configured with multiple domain IDs by using the **domain-id secondary** command, but there is only one primary domain ID, and others are secondary domain IDs. When the conversion from the OSPF

route to the VPN route is announced, the related extended community attribute also carries the primary domain ID information only.

Generally, the OSPF protocol runs between PE and CE to exchange VPN routes. After receiving the VPN route and redistributing it to the OSPF instance, PE announces this to the VPN site as type 5 LSA. However, for different sites that belong to one OSPF domain, the route should be announced as type 3 LSA. Therefore, after the same domain ID is configured for the related VRF OSPF instance on the PE, the route inside the domain can be announced as type 3 LSA.

In one PE, domain IDs of different VRF OSPF instances do not affect each other. They can be the same or different. The VRF OSPF instances that belong to one VPN should be configured with the same domain ID to ensure correct route announcement.

Examples

Configure the domain ID of the VRF OSPF instance.

```
DES-7200(config)# router ospf 10 vrf vpn1
DES-7200(config-router)# domain-id type 0005 value 000000000001
```

Related commands

Command	Description
show ip ospf	Show the summary information of the OSPF instance.

2.1.13 domain-tag

Use this command to configure the VPN domain-tag of the OSPF instance associated with the VRF. The **no** command restores the default value of the VPN domain-tag of the OSPF instance.

domain-tag *tag*

no domain-tag

Parameter description

Parameter	Description
tag	The domain-tag value of the OSPF instance, ranging from 1 to 4294967295

Default configuration

The default value of the VRF OSPF instance is the AS number of the local BGP protocol.

Command mode	OSPF Router mode
Usage guidelines	This command is valid only for the OSPF instance associated with the VRF, and only for the BGP redistributed route. If a VPN site connects multiple PEs, the VPN site learns the VPN route through MP-BGP from PEs. If the VPN route is announced to the VPN site through type 5 or type 7 LSA which may be learned by other PE routers connected to the VPN site and advertised, a loop may come into being. To prevent such a loop, configure the same VPN domain-tag for the VRF OSPF instances connected to the same VPN site on a PE. When the VRF OSPF instance sends type 5 or type 7 LSA to the VPN site, the LSA is attached with the VPN domain-tag information. When other PE sites receive type 5 or type 7 LSA, if the VPN domain-tag in the LSA is identical to the VPN domain-tag of the local OSPF instance, the LSA does not participate in OSPF calculation. Generally, the OSPF instances that belong to the same VPN should be configured with the same tag value. The VPN domain-tag contains four bytes in the OSPF packet. If this command is not configured for the VRF OSPF instance, by default, when the OSPF instance announces type 5 or type 7 LSA, the former two bytes of the VPN domain-tag are set to 0xD000, and the latter two bytes are set to the AS number of the local BGP. For example, if the AS number of the local BGP is 1, the hexadecimal value of the VPN domain-tag is 0xD0000001.

Examples	Set the domain-tag value of the OSPF instance to 10.
	`DES-7200(config)# router ospf 10 vrf vpn1`
	`DES-7200(config-router)# domain-tag 10`

Related commands

Command	Description
capability vrf-lite	Enable/Disable loop inspection.

2.1.14 export map

Use this command to define the policy rule of exporting extended community attribute from local VRF to remote VPN route.

[**no**] **export map** *routemap-name*

Parameter description

Parameter	Description
routemap-name	Associated route map policy rule.

Default configuration

By default, no policy rule of extended community attribute is exported.

Command mode

VPN configuration mode

Usage guidelines

This command allows you to more precisely control the extended group attribute of an exported route. You are allowed to add or modify the extended community attribute defiend by the **route-target export** command. The route map assocaited by this command supports two rules only: match IP address and set extcommunity.

Examples

To configure the extended group attribute associated with rma on VPNA, use the following command:

```
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# export map rma
```

Related commands

Command	Description
route-target	Define the import and export RT policy of VRF.

2.1.15 exit address-family

Use this command to exit the VRF address family configuration or vpn address family configuration mode.

exit address-family

Command mode	Specific address family configuration mode

Examples

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# exit address-family
```

2.1.16 extcommunity-type

Use this command to configure router-id or route-type of the OSPF instance associated with the VRF. The **no** command restores the default value.

extcommunity-type {**router-id** {**0107|8001**} **| route-type** {**0306|8000**}}

no extcommunity-type {**router-id | route-type** }

Parameter description

Parameter	Description
router-id {**0107|8001**}	Set the router-id type of the OSPF instance. The value can be 0107 or 8001.
route-type {**0306|8000**}	Set the route-type type of the OSPF instance. The value can be 0306 or 8000.

Default configuration	By default, the router-id type is 0107, and the route-type type is 0306.
Command mode	OSPF Router mode
Usage guidelines	The command is valid only for the OSPF instance associated with the VRF, and not valid for the global VRF instance. When the OSPF route of VRF forms the VPN route, the extended community attribute of the VPN route also carries the router-id information of the OSPF instance. The type field value of the extended community attribute can be set to 0x0107 or 0x8001 by running the **extcommunity-type router-id** command. When the OSPF route of VRF forms the VPN route, the extended community attribute of the VPN route can also carry the router-type information of the OSPF instance. The type field value of the extended community attribute can be set to 0x0306 or 0x8000 by running the

extcommunity-type router-type command.

Examples

Set router-id of the OSPF instance to 8001.

```
DES-7200(config)# router ospf 10 vrf vpn1
DES-7200(config-router)# extcommunity-type router-id 8001
```

Related commands

Command	Description
-	-

2.1.17 import map

Use this command to define the policy rule of importing remote VPN routes to local VRF.

[**no**] **import map** *routemap-name*

Parameter description

Parameter	Description
routemap-name	Associated route map policy rule.

Default configuration

By default, no import policy rule is defined.

Command mode

VPN configuration mode

Usage guidelines

This command allows you to more precisely control the import of remote VPN route to local VRF . The rule defiend by the **import map** command takes effect after the import of extended community attribute deinfed in the VRF. Namely, the rule defined by this command filters the received remote VPN routes only when they match the extended community attribute defiend by the **route-target import** command in the VRF. The route map assocaited by this command supports two rules only: match IP address and match extcommunity.

Examples

To configure the extended group attribute associated with rma on VPNA, use the following command:

```
DES-7200(config)# ip vrf VPNA

DES-7200(config-vrf)# import map rma
```

Related commands

Command	Description
route-target	Define the import and export RT policy of VRF.

2.1.18 ip extcommunity-list

Use this command to define the extended community list referred in the route map, which is used to filter VPN routes in BGP/MPLS VPN applications. Use the **no** form to delete the extended community list.

ip extcommunity-list {*expanded-list* **| expanded** *list-name* **} {permit | deny}** *[regular-expression]*

ip extcommunity-list {*standard-list* **| standard** *list-name* **} {permit | deny} [rt** *value***] [soo** *value***]**

no ip extcommunity-list {*expanded-list* **| expanded** *list-name* **|** *standard-list* **| standard** *list-name* **}**

Use the following command to define the extended community list created by name. Use the no form to delete the extended community list.

ip extcommunity-list {*expanded-list* **| expanded** *list-name* **|** *standard-list* **| standard** *list-name* **}**

no ip extcommunity-list {*expanded-list* **| expanded** *list-name* **|** *standard-list* **| standard** *list-name***}**

The command in the expanded ip extcommunity-list configuration includes:

[no] [*sequence-number***]deny** *regular-expression*

[no] [*sequence-number***] permit** *regular-expression*

exit

The command in the standard ip extcommunity-list configuration includes:

[no] [*sequence-number***] deny {[rt** *value*] [**soo** *value*]**}**

[no] [*sequence-number***] permit {[rt** *value*] [**soo** *value*]**}**

exit

Parameter description

Parameter	Description
expanded-list	Value range (100-199), which is used to identy extended extcommunity list. One extcommunity list can contain multiple rules.
standard-list	Value range (1-99), which is used to identy standard extcommunity list. One extcommunity list can contain multiple rules.
expanded *list-name*	Name of extended extcommunity list less than 32 characters. This parameter allows you to enter the extended community list configuration mode.
standard *list-name*	Name of standard extcommunity list less than 32 characters. This parameter allows you to enter the standard community list configuration mode.
permit	Define an extcommunity permit rule.
deny	Define an extcommunity deny rule.
regular-expression	(optional) Define the template to match extcommunity.
sequence-number	(Optional) Sequence number of a rule in the range 1 to 2147483647. Without specification, by default when a rule is added, its sequence nubmer automatically increases by 10 starting with 10.
rt	(Optional) Set RT, which can be used only for standard extcommunity configuration.
soo	(Optional) Set SOO, which can be used only for standard extcommunity configuration.
vlue	RT or SOO value

Default configuration

By default, no extended community is deifned.

Command mode

Global configuration mode and ip extcommunity-list configuration mode

Usage guidelines

The **ip extcommunity-list** command is used to create an extcommunity list including multiple extcommunity values, which is mainly applied for the match extcommunity rule of route map to match the extended community of BGP routes for route filtering.

For definition of extended extcommunity, the principle of regular-expression is as follows:

Symbol	Description
.	Match any single character.
*****	Match zero or any sequence in the character string.
+	Match one or any sequence in the character string.
?	Match zero or one symbol in the character string.
^	Match the starting of the character string.
$	Match the ending of the character string.
_	Match the comma, bracket, starting and ending of the character string, and space.
[ ]	Match the single character in a certain range.

Examples

Define ip extcommunity-list.

```
DES-7200(config)# ip extcommunity-list 1 permit rt 100: 1
DES-7200(config)# ip extcommunity-list standard aaa permit rt
100: 2
DES-7200(config)# ip extcommunity-list expanded ext1 permit 200:
[0~9][0~9]
```

Use ip extcommunity.

```
DES-7200(config)# route-map rt_in_filter
DES-7200(config-route-map)# match extcommunity 1
```

Examples

```
DES-7200(config-route-map)# match extcommunity ext1
DES-7200(config)# router bgp 100
DES-7200(config-router)# address-family vpn
DES-7200(config-router-af)#neighbor 3.3.3.3 send-community extended
DES-7200(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in
```

Related commands

Command	Description
match extcommunity	Match extcommunity.

2.1.19 ip route static inter-vrf

Use this command to enable or disable the static inter-vrf route.

[no] ip route static inter-vrf

Default configuration Enable the static inter-vrf route by default.

Command mode Global configuration mode

Usage guidelines If users configure the **no ip route static inter-vrf**, the inter-vrf route of static configuration will not be valid. If the active static inter-vrf route is existed, when you configure it again, it will print similar information as follow, to prompt to delete the static inter-vrf route.

*Aug 7 10:58:34: %NSM-6-ROUTESACROSSVRF: **Un-installing route** [*x.x.x.x/8*] **from global routing table with outgoing interface** *x/x.*

Examples

```
DES-7200(config)# no ip route static inter-vrf
```

2.1.20 ip route vrf

Use this command to create a static routing table entry for the VFR. Use the **no** form of this command to delete the entry.

[**no**] **ip route vrf** *vrf-name ip-addr mask interface next-hop-address* [**global**]

Parameter description

Parameter	Description
vrf-name	VRF name.
ip-addr	Prefix of the destination address of the route
mask	Mask of the prefix of the destination address
interface	Egress of the destination address.
next-hop	Next hop of the destination address
global	Indicate the next hop is of the global VRF.

Default configuration

There is no static route by default.

Command mode

Global configuration mode

Usage guidelines

The outgoing interface can be specified to bind to the interface of other vrf, to configure the static inter-VRF route. If the global parameter is configured, it is considered as the route of the global VRF. However, if the interface and global parameter are configured at the same time, and the interface is not within the global vrf, it will take the vrf where the interface locates as the standard.

Note: Configure the global to cross the global inter-vrf. It is not limited by the **no ip route static inter-vrf** command.

Examples

```
DES-7200(config)# ip route vrf vrf1 10.10.10.0 255.255.255.0 gi3/1
192.168.18.1
```

2.1.21 ip vrf

Use this command to create a VRF. Use the **no** form of this command to delete a VRF.

[**no**] **ip vrf** *vrf_name*

Parameter description

Parameter	Description
vrf_name	VRF name.

Default configuration

By default, no vrf is defined.

Command mode

Global configuration mode

Examples

```
DES-7200(config)# ip vrf vrf1
```

Related commands

Command	Description
ip vrf forwarding	Bind the VRF with an interface
show ip vrf	Show VRF configurations.
rd	Configure the RD for the VRF
route-target	Configure the RT attribute for the VRF.

2.1.22 ip vrf forwarding

Use this command to bind the VRF with an interface. Use the **no** form of this command to remove the binding.

[**no**] **ip vrf forwarding** *vrf-name*

Parameter

Parameter	Description

description	*vrf-name*	VRF name.

Default configuration

By default, the VRF is not binding with any interface.

Command mode

Interface configuration mode

Examples

```
DES-7200(config)# int eth1
DES-7200(config-if)# ip vrf forwarding vrf1
```

Related commands

Command	Description
ip vrf	Create a VRF instance
show ip vrf	Show the VRF configurations

2.1.23 match extcommunit

Use this command to define the rule of matching the extended community of BGP in the route map configuration mode. Use the no form to remove the setting.

match extcommunity *{standard-list-number|standard-list-name|expanded-list-num|expanded-list-name}*

no match extcommunity *{standard-list-number|standard-list-name|expanded-list-num|expanded-list-name}*

Parameter description

Parameter	Description
expanded-list-num	In the range 100 to 199, which is used to identy extended extcommunity list. One extcommunity list can contain more than one rule.

expanded-list-nam	Name of extended extcommunity list. One extcommunity list can contain more than one rule.
standard-list-num	In the range 1 to 99, which is used to identy standard extcommunity list. One extcommunity list can contain more than one rule.
standard-list-nam	Name of standard extcommunity list. One extcommunity list can contain more than one rule.

Default configuration

By default, no match rule is deifned.

Command mode

Route map configuratin mode

Usage guidelines

Two kidns of route mpas have the rule of matching extended community:

1. Route map associated by the **import map** command, which uses RT to filter the routes imported into the VRF.
2. Route map associated by the **neighbor route-map in** and **neighbor route-map out** commands configured in the VPNv4 address family configuration mode, which uses RT to filter VPNv4 routes from/to BGP peers.

Examples

Define two extended communities.

```
DES-7200(config)# ip extcommunity-list 1 permit rt 100: 1
DES-7200(config)# ip extcommunity-list 1 permit rt 100:2
```

Define match rule in the route map.

```
DES-7200(config)# route-map rt
DES-7200(config-route-map)# match extcommunity 1
```

Use the route map.

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 3.3.3.3 route-map rt in
```

Related commands

Command	Description
ip extcommunity-list	Creatge extended community list.
show ip extcommunity-list	Show extended community list.

2.1.24 match mpls-label

Use this command to receive the routes matching label from the BGP peer. Use the no form to remove the setting.

match mpls-label

no match mpls-label

Default configuration

By default, no match rule is deifned in the associated route map policy.

Command mode

Route map configuratin mode

Usage guidelines

This command applies to only the route map associated by the **neighbor route-map in** command, which is used to only filter the inbounding routes received from the BGP peer. If the rule defined in the route map has not this command, the route are permitted as long as they match other rules, no matter whether they are tagged or not.

Note that this command takes effect for tagged IPv4 routes, not VPNv4 routes.

Examples

Create a route map and receive the routes matching the following conditions:

1 The route prefix matches the rule defined ACL 1.

2 The route has MPLS label.

```
DES-7200(config)# route-map infilter permit 10
DES-7200(config-route-map)# match ip address acl1
DES-7200(config-route-map)# match mpls-label
DES-7200(config-route-map)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 1.1.1.1 route-map infilter in
```

Related commands

Command	Description
neighbor send-label	Exchange the routes of MPLS label between the BGP peers.
neighbor route-map out	Control the routes to the BGP peer.
neighbor route-map in	Control the routes received from the BGP peer.
set mpls-label	Assign MPLS label to permitted routes.

2.1.25 maximum routes

Use this command to limit the maximum routes within the vrf. Use the **no** form of this command to cancel this limit.

maximum routes *limit* {*warn-threshold* **| warning-only**}

no maximum routes

Parameter description

Parameter	Description
limit	Limit the routes. The routes which exceed the limits will not be written into the core route table, ranging from 1 to 4294967295.
warn-threshold	Print the warning threshold, It will print the warning after the percent is reached, ranging from 1 to 100.
warning-only	After the configured limit is reached, it only prints the warning. But it is still allowed to add to the core route table.

Default configuration	There is no limit for the configuration by default.
Command mode	VRF configuration mode
Usage guidelines	Use this command to limit the allowed routes within the VRF. If it only hopes to get the warning, use the warning-only parameter.
Examples	DES-7200(config)# **ip vrf** *vrf1* DES-7200(config-vrf)# **rd** *200:1* DES-7200(config-vrf)# **maximum routes** *1000* **warning-only**

2.1.26 neighbor activate

Use this command to activates the neighboring or peer group under current address mode. Use the **no** form of this command to restore the default value.

neighbor {*peer-address* | *peer-group-name*} **activate**

no neighbor {*peer-address* | *peer-group-name*} **activate**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer. This address can be the IPv4 or IPv6 address.
peer-group-name	Specify the name of the peer group. The peer group name doesn't exceed 32 characters.

Default configuration	It is enabled under the address family IPv4.

Command mode	The BGP configuration mode, the IPv4 address family configuration mode of BGP, the IPv6 address family configuration mode of BGP, the IPv4 VRF configuration mode of BGP and the VPNv4 address family configuration mode of BGP.
Usage guidelines	For the address family of ipv4, this function is enabled by default. For other address family type, you need to configure this command for route information exchange.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 100
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 10.0.0.1 activate
```

Related commands

Command	Description
router bgp	Open the BGP protocol.
neighbor remote-as	Configure the peer of BGP

2.1.27 neighbor allowas-in

When you configure the PE, you can use this command to allow the PE to receive the messages with AS numbers duplicated with this PE. Use the **no** form of this command to restore the default value.

neighbor {*peer-address* | *peer-group-name*} **allowas-in** *number*

no neighbor {[*peer-address* | *peer-group-name*} **allowas-in**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.
number	The repeated times of the allowed AS

		number. The default value is 3. The range is within [1, 10].

Default configuration	By default, the allowas-in function is not enabled
Command mode	BGP VPN address-family configuration mode, IPv4VRF address family configuration mode of BGP
Usage guidelines	The typical application is in the spoke-hub model. Configure this command on the PE so that the PE can receive and send the advertised address prefix. Configure two VRFs on the PE. Set one of them to receive the route information of all PEs, and notify it to the CE; the other vrf receives the route information advertised by the CE and advertises them to all the PEs. You can make settings at both the IBGP peer and EBGP peer.
Examples	DES-7200(config)# **router bgp** *60* DES-7200(config-router)# **neighbor** *10.0.0.1* **remote-as** *100* DES-7200(config-router)# **address-family ipv4 vrf** *vpn1* DES-7200(config-router-af)# **neighbor** *10.0.0.1* **allowas-in**

Related commands

Command	Description
router bgp	Open the BGP protocol.
neighbor remote-as	Configure the peer of the BGP.

2.1.28 neighbor as-override

Use this command to configure the PE to cover the AS number of a site. Use the **no** form of this command to restore the default value.

neighbor {*peer-address* | *peer-group-name*} **as-override**

no neighbor {*peer-address* | *peer-group-name*} **as-override**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.

Default configuration

By default, the as-override function is not enabled.

Command mode

IPv4VRF address family configuration mode of BGP

Usage guidelines

Normally, the BGP protocol will not receive the route information with the same AS number as the AS. You can use this command to cover the AS number so that the BGP protocol can receive the route information from the same AS number.

In the VPN, the most typical application lies in that the two CE ends have the same AS number. Normally, these two CEs cannot receive the other from the other party. After the above command is configured on the PE, you can let the PE cover the AS number of the CE so that the CE from the other end can receive the route information.

Only set this function for the EBGP peer.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 100
DES-7200(config-router)# address-family ipv4 vrf vpn
DES-7200(config-router-af)# neighbor 10.0.0.1 as-override
```

Related commands

Command	Description
router bgp	Enable BGP protocol

	neighbor remote-as	Configure the peer of BGP

2.1.29 neighbor description

Use this command to set the descriptive language for specified peer (group). Use the **no** form of this command to cancel this configuration.

neighbor {*peer-address* | *peer-group-name*} **description text**

no neighbor {*peer-address* | *peer-group-name*} **description**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.
text	Use to describe the text of this peer (group). Range: up to 80 characters.

Default configuration

Disabled.

Command mode

BGP configuration mode, IPv4VRF address family configuration mode of BGP

Usage guidelines

Use this command to add the descriptive character for the peer (group).It can help us remember the characteristics and features of this peer (group) better.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.1.1.1 remote-as 80
DES-7200(config-router)# neighbor 10.1.1.1 description xyz.com
```

Related commands

Command	Description
router bgp	Enable BGP protocol
neighbor remote-as	Configure the peer (group) of BGP.

2.1.30 neighbor next-hop-self

Use this command to modify the next hop as itself when sending routes to the peer. Use the **no** form of this command to cancel this configuration.

neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

no neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group less than 32 characters.
next-hop-self	Modify the next hop as itself when sending routes to the peer

Default configuration

By default, the next hop is not modified when sending routes to the peer.

Command mode

BGP configuration mode, IPv4 and VPNv4 address family configuration modes of BGP

Usage guidelines

In the inter-domain VPN OptionB solution, use this command in the BGP VPN address configuration mode to modify the enxt hop.

Examples

```
DES-7200(config)# router bgp 60
```

```
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 10.1.1.1 next-hop-self
```

Related commands

Command	Description
router bgp	Enable BGP protocol.
neighbor remote-as	Configure the peer (group) of BGP.

2.1.31 neighbor next-hop-unchanged

Use this command to maintain the next hop when sending routes to the peer. Use the **no** form of this command to cancel this configuration.

neighbor {*peer-address* | *peer-group-name*} **next-hop-unchanged**

no neighbor {*peer-address* | *peer-group-name*} **next-hop- unchanged**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group less than 32 characters.
next-hop-unchanged	Maintain the next hop when sending routes to the peer

Default configuration

By default, the next hop is not modified when sending routes to the peer.

Command mode

BGP configuration mode, IPv4 and VPNv4 address family configuration modes of BGP

Usage guidelines	In the inter-domain VPN OptionC (Multihop MP-EBGP) solution, you can set one route reflector in each AS to reduce the conenctions of PEs of inter-domain VPN. The route reflectors in different ASs set up Multihop MP-EBGP connectons to exhcnage VPN routes. By default, the next hop is changed as itself when the route reflector sends routes to the EBGP peer. Consequently, when PEs in other ASs receive VPN routes, they consider the next hop of VPN routes to be the route reflector. In this way, all inter-domain VPN traffic passes through the route reflector. This is not the optimal forwarding path and imposes higher demand on the forwarding of RR. To avoid this circumstnace, when the route reflector establishes inter-domain Multihop MP-EBGP connection, run the **neighbor next-hop-unchanged** command in the VPNv4 address family mode to maintain the next hop of VPNv4 routes.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 10.1.1.1 next-hop-unchanged
```

Related commands

Command	Description
router bgp	Enable BGP protocol.
neighbor remote-as	Configure the peer (group) of BGP.

2.1.32 neighbor remote-as

Use this command to configure the peer (group) of BGP. Use the **no** form of this command to delete the configured peer (group).

neighbor {*peer-address* | *peer-group-name*} **remote-as** *as-number*

no neighbor {*peer-address* | *peer-group-name*} **remote-as**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer, which may be the IPv4 or IPv6 address.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.

	as-number	AS number of the BGP peer (group). The range is from 1 to 65535.

Default configuration

No BGP peer is configured.

Command mode

BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP

Usage guidelines

If you specify the BGP peer group, all members of the peer group will inherit the setting of this command.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 80
```

Related commands

Command	Description
router bgp	Enable BGP protocol

2.1.33 neighbor send-label

Use this command to exchange the IPV routes of MPLS label with the peer (group). Use the **no** form of this command to disable this funciton.

neighbor {*peer-address* | *peer-group-name*} **send-label**

no neighbor {*peer-address* | *peer-group-name*} **send-label**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.

	peer-group-name	Specify the name of the peer group of less than 32 characters.
	send-label	Send IPv4 routes of MPLS label to the BGP peer (group).

Default configuration	No routes of MPLS label is sent to the BGP peer.

Command mode	BGP configuration mode, IPv4 address family configuration mode of BGP

Usage guidelines

This command must be configured on the local rotuer and the adjacent router. If the BGP session is set up, this configuration takes effect after the BGP session resets.

To enable distribution of labels for IPv4 routes on the IBGP session, use the **neighbor** *{peer-address|peer-group_name}* **update-source loopback** *id* command to set the the loopback address as source address of the BGP session. If you use the IP address of the direct interface as the source address, the LDP will distribute label-3 to its upstream devices for the connected P device considers the direct route to be egress. In this way, the LSP tunnel is terminated on the PE device, not the PE. Consequently, to use the loopback address (generally 32-bit mask) to identify the PE itself, ensure that the egress of LSP is the PE. For direct EBGP session, you do not need to bind the loopback address. Instead, you can use the IP address of direct interface as the soruce address of EBGP session. For the single-hop direct EBGP session which enables BGP route (IPv4 route or VPN route) to carry with label, MP-BGP automatically genertes a host route of 32-bit mask to the egress (namely EGBGP neighbor address) to prevent LSP from being terminated in advance for the host address is aggregated by the direct route. At this time, the LDP will not send label-3 to its upstream through the host route of EBGP neighbor address for it does not consider itself to be the egress.

Caution

When you use BGP as the label distribution protocol, run the label-switching command on the interface on which MPLS message is forwarded to enalbe the label forwarding capability.

Examples

Send IPv4 route of MPLS label to 10.10.10.1.

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# neighbor 10.0.0.1 remote-as 65501
DES-7200(config-router)# neighbor 10.0.0.1 update-source loopback 0
DES-7200(config-router)# neighbor 10.0.0.1 send-label
```

Related

Command	Description

neighbor route-map in	Set the policy of receiving routes from the peer.
neighbor route-map out	Set the policy of sending routes to the peer.
label-switching	Enable the label forwarding capability on the interface.
match mpls-label	Match the MPLS label defiend in the route map.
set mpls-label	Distribute the MPLS lable to the routes matching the route map.

2.1.34 neighbor shutdown

Use this command to disable the BGP connection established for specified BGP peer. Use the **no** form of this command to restart the BGP peer (group).

neighbor {*peer-address* | *peer-group-name*} **shutdown**

no neighbor {*peer-address* | *peer-group-name*} **shutdown**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer, which can be the IPv4 or IPv6 address.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.

Default configuration

Disabled.

Command mode

BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP

Usage guidelines

Use this command to disable the valid connection established for specified peer (group), and delete all associated route information.However, this command still remains the configuration information of this specified peer (group).

If you specify the BGP peer group, all members of the peer group will inherit the setting of this command. However, if you set this command for some member of the peer, it will cover the peer group-based setting.

Examples

```
DES-7200(config)# router bgp 60
DES-7200(config-router)# neighbor 10.0.0.1 shutdown
```

Related commands

Command	Description
router bgp	Enable BGP protocol
neighbor remote-as	Configure the peer of BGP
show ip bgp summary	Show the connection status of BGP

2.1.35 neighbor soo

Use this command to configure the neighbor source site attribute value. Use the **no** form of this command to cancel the neighbor source site attribute value.

neighbor {*peer-address* | *peer-group-name*} **soo soo-value**

no neighbor {*peer-address* | *peer-group-nam*e} **soo**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.
soo-value	Value of soo. soo-value can have two different kinds of parameters: (1)soo-value= as-num:nn

		an-num is the puclic autonomous area system number, and nn is specified by the user (2)soo-value = ip-addr:nn The ip-addr address must be a global IP address, and nn is specified by the user

Default configuration

By default, the soo function is not enabled.

Command mode

BGP IPv4 address family configuration mode

Usage guidelines

In the CE model, this command prevents the route information from the CE to the PE to return to the CE end.

Examples

```
DES-7200(config)# router bgp 65000
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router-af)# neighbor 10.0.0.1 remote-as  100
DES-7200(config-router-af)# neighbor 10.0.0.1 soo 100:100
```

Related commands

Command	Description
router bgp	Enable BGP protocol

2.1.36 rd

Use this command to define the RD value of the VRF

rd *rd-value*

Parameter description

Parameter	Description
rd_value	The RD value.

Default configuration	By default, no RD value is configured. The default RD value is 0:0.
Command mode	VRF configuration mode.
Usage guidelines	If you have defined a VRF and configured the RD value for it, you cannot modify the RD value. If it is absolutely necessary to modify the RD value, the only way is to first delete the VRF and then configure the RD value for it. One VRF can have only one RD value, and you cannot define multiple RD values for it.
Examples	`DES-7200(config)# ip vrf vrf1` `DES-7200 (config-vrf)# rd 100:1`

Related commands

Command	Description
ip vrf	Create a VRF instance
show ip vrf	Show the VRF configuration

2.1.37 recursive-route lookup lsp

Use this command to enable the capability of resolving the next hop of the BGP route to the LSP tunnel, and the no command disables this capability.

recursive-route lookup lsp
no recursive-route lookup lsp

Parameter description

Parameter	Description
-	-

Default configuration	Disable the capability of resolving the next hop of the BGP route to the

	LSP tunnel.

Command mode	Global configuration mode

Usage guidelines	By default, the next hop of the BGP route without a tag is not resolved to the LSP tunnel. In a CSC application scenario, for the model where level 2 carriers provide Internet services based on the IP core, the next hop of the BGP route must be resolved to the LSP tunnel in the CSC CE by running this command.

Examples	Enable the capability of resolving next hop of the BGP route to the LSP tunnel. `DES-7200(config)# recursive-route lookup lsp`

Related commands

Command	Description
-	-

Platform description	None

2.1.38 redistribute

The route redistributed command can be used to carry out the redistribution between the route information of other route protocol and BGP, and the no form of this command can be used to delete this function and its parameter configuration.

redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

no redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

Parameter description

Parameter	Description
protocol-type	Type of source protocol for the redistributed route. There are connected, static and rip protocol at present.

route-map *map-tag*	The name of the associate **route-map**. No associate with **route-map** by default.
metric *metric-value*	The default metric value of the configured redistribution route. This value is not set by default.

Default configuration

Disabled

Command mode

BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP

Usage guidelines

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time. The switches can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

Description: When the no command is configured, if the parameters are configured and there are corresponding parameter configurations, it will cancel the configuration of corresponding parameters.If there is no parameter, this configuration of redistribute will be canceled.

Caution: for the metric value of the route, it will apply the route-map to process according to original value. If it is processed in the route-map, it will use the value after the route-map process. If this value is not set in the route-map, but the metric option is configured, it will use the metric configuration value. If there is not any value, it will use the redistributed value.

Examples

```
DES-7200(config-router)# redistribute static route-map static-rmap
DES-7200(config-router)# no redistribute static
route-map static-rmap
DES-7200(config-router)# no redistribute static
```

Related commands

Command	Description
show ip protocols	Show the protocol configuration.

2.1.39 redistribute OSPF

The route redistributed command can carry out the redistribution between the route information of the OSPF route protocol and BGP, and the no form of this command can be used to delete this function and its parameter configuration.

redistribute ospf *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [**1**|**2**] **nssa-external** [**1**|**2**]]

no redistribute ospf *process-id* [**route-map** *map-tag*] [**metric**] **[match {internal|external [1|2]|nssa-external [1|2]}]**

Parameter description

Parameter	Description
process-id	Process ID of the redistributed OSPF protocol.
route-map *map-tag*	The name of the associate **route-map.** No associated with **route-map** by default.
metric *metric-value*	Configured default metric value of the redistributed route. This value is not set by default.
match	Used to set the matched subtype of the OSPF route.
internal	Internal subtype of route for OSPF, the default configuration of match item for the redistributed ospf route.
external [**1**|**2**]	External type of route for OSPF, can describe the type 1 or type 2 in detail. If not specified, it includes the type 1 and type 2.
nssa-external [**1**|**2]**	nssa-external type of route for OSPF, can describe the type 1 or type 2 in detail. If not specified, it includes the type 1 and type 2.

Default configuration

Disable the redistributed OSPF route.

Command mode

BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP

Usage guidelines

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time. The switches can run the protocols at the same time, so it should redistribute the protocols.

Note

When the no command is configured, if the parameters are configured and there are corresponding parameter configurations, it will cancel the configuration of corresponding parameters.If there is no parameter, this configuration of redistribute will be canceled. When all of the route subtypes are deleted, it is the default route type.

Caution

The filtration rule of the OSPF route is to carry out the filtration of the OSPF route type according to the configured match option, and then carry out the filtration of the route-map rule.For the metric value of the route, it will carry out the route-map process according to the redistributed metric value. If it is processed in the route-map, it will use the value after the route-map process. If it is not processed in the route-map, but the metric option is configured, it will use the metric configuration value. If there is no any value, it will use the redistributed value directly.

Examples

```
DES-7200(config-router)# redistribute ospf 2 route-map static-rmap
DES-7200(config-router)# no redistribute ospf 4 match external route-map
ospf-rmap
DES-7200(config-router)# no redistribute ospf 78
```

Related commands

Command	Description
show ip protocols	Show the protocol configuration.

2.1.40 route-target

Use this command to define or cancel the RT attribute of a VRF.

[**no**] **route-target** {**import | export | both**} *rt-value*

Parameter description

Parameter	Description
import	Set the import value for the VRF
export	set the export value for the VRF
both	Set the import and export value for the VRF

Default configuration

By default, no Route-Target is defined.

Command mode

VRF configuration mode

Usage guidelines

In one VRF, you can configure multiple import and expoer route-target attribute values.

Examples

```
DES-7200(config)# ip vrf vrf1
DES-7200(config-vrf)# route-target import 100:1
DES-7200(config-vrf)# route-target export 100:2
DES-7200(config-vrf)# route-target both 100:4
```

Related

Command	Description

	ip vrf	Create a VRF instance

2.1.41 set extcommunit

Use this command to set the extended community in the route map configuration mode. Use the **no** form to remove the setting.

set extcommunity {rt *extended-community-value* **[additive] | soo** *extended-community-value***}**

no set extcommunity {rt | soo}

Parameter description

Parameter	Description
rt	Set RT value.
soo	Set SOO value.
additive	(Optional) Add new RT attribute to the RT list, not replacing any existing RT attributes.
extended-community-value	Extended community value. You can set multiple RT values separate by space, but only one for SOO.

Default configuration

By default, this rule is not defined in associated route map policy. Without additive, this command will replace all RT lists.

Command mode

Route map configuratin mode

Usage guidelines

This command applies to the following circumstances:

1. Route map associated by the **export map** command, which controls the extended community of VPN routes based on policy.
2. Route map associated by the **neighbor route-map out** commands configured in the VPNv4 address family configuration mode, which modifies received and sent VPNv4 routes.

Without additive, the **set extcommunity rt** command replaces the original RT value with the set one. With addtivie, the command addes the new set RT value.

Without SOO attribute in the extended community attribute list of BGP route, the **set extcommunity soo** command adds the SOO attributes. With SOO attribute, the command replace the original SOO value with the set one.

Examples

```
DES-7200(config)# route-map set-rt
DES-7200(config-route-map)# set extcommunity rt 100:1 200:1
DES-7200(config-route-map)# exit
DES-7200(config)# ip vrf vrf1
DES-7200(config-vrf)# export map set-rt
```

Related commands

Command	Description
match extcommunity	Match the extended community attribute.

2.1.42 set mpls-label

Use this command to distribute MPLS label to the routes matching the route map. Use the **no** form to remove the setting.

set mpls-label

no set mpls-label

Default configuration

By default, the IPv4 routes are sent to the BGPpeer without MPLS label.

Command mode

Route map configuratin mode

Usage guidelines

This command applies to only the route map associated by the **neighbor route-map out** command, which is used to only filter the outbounding routes sent to the BGP peer.

This command takes effect in the route map only after using the **neighbor send-label** command to enable exhange of the routes of MPLS label between the BGP peers. Othewise, the command distributes the routes matching the route map without label. On the other hand, if you use the **neighbor send-label** command to enable exhange of the routes of MPLS label between the BGP peers, but does not ocnfigure the **set mpls-label** command on the associated route map, only the IPv4 routes matching the route map are distributed without MPLS label.

Examples

Create a route map, distribute MPLS label to the route of 1.1.1.1/32 prefix, distribute general IPv4 route update without MPLS label to the route of 1.1.1.2/32 prefix, but distribute no rotue update to the routes that do not match ACL1 and ACL2.

```
DES-7200 (config)# ip access-list standard acl1
DES-7200 (config-std-nacl) # permit host 1.1.1.1
DES-7200 (config-std-nacl) # exit
DES-7200 (config)# ip access-list standard acl2
DES-7200 (config-std-nacl) # permit host 1.1.1.2
DES-7200 (config-std-nacl) # exit
DES-7200 (config)# route-map out-as permit 10
DES-7200 (config-route-map)# match ip address acl1
DES-7200 (config-route-map)# set mpls-label
DES-7200 (config-std-nacl) # exit
DES-7200 (config)# route-map out-as permit 20
DES-7200 (config-route-map)# match ip address acl
```

Related commands

Command	Description
neighbor send-label	Exchange the routes of MPLS label between the BGP peers.
neighbor route-map out	Control the routes to the BGP peer.
match mpls-label	Receive only the routes of MPLS label from the BGP peer.

show ip bgp labels	Show the routes of MPLS label that the BGP learns and sends.

2.2 Showing Commands

2.2.1 show bgp ipv4 unicast labels

Use this command to show the routes of MPLS labels that the BGP learns and sends.

show bgp ipv4 unicast labels

Default configuration

N/A.

Command mode

Privileged mode.

Usage guidelines

This command shows IPv4 routes of MPLS label. To show the VPNv4 routes of MPLS label, run the **show bgp vpnv4 unicast** command.

Examples

```
DES-7200 #show bgp ipv4 unicast labels
Network         Next Hop        In Label/Out Label
1.1.1.1/32      192.167.1.1     17/18
1.1.1.2/32      192.167.1.1     nolabel/19
```

Field	Description
Network	Route prefix
Nexthop	Next hop of the route
In label	The label that the local router assigns (if available)
Out label	The label learned from the next hop router of the route (if existent)

Related commands

Command	Description
neighbor send-label	Exchange the routes of MPLS label between the BGP peers.
show bgp vpnv4 unicast	Show the label informaiton of VPN routes.

2.2.2 show bgp vpnv4 unicast

Use this command to show the VPN route information.

show bgp vpnv4 unicast all [*network* | **neighbor** [*peer-address*] | **summary** | **label**]

show bgp vpnv4 unicast vrf *vrf_name* [*network* | **summary** | **label**]

show bgp vpnv4 unicast rd *rd_value* [*network* | **neighbor** [*peer-address*] | **summary** | **label**]

Parameter description

Parameter	Description
network	Show the prefix of the specified destination network.
neighbor [*peer-address*]	Show the neighbor information of the specified VPN.
summary	Show the state of the BGP peer.
label	Show the label information of the route.
all	Show the VPN route information of all VRFs.
vrf_name	Show the VPN route information of the specified VRF.
rd_value	Show the VPN route information of the specified RD value.

Default configuration N/A.

Command mode

Privileged mode.

Usage guidelines

This command allows you to show the VPN route information. For the BGP/MPLS VPN application environment, the routes of BGP VRF instnaces are elected and imported by MP-BGP. Hence, this command shows only elected routes. The detailed MP-BGP route information should be viewed in the **show bgp vpnv4 unicast all** command.

Examples

```
DES-7200# show bgp vpnv4 unicast all

Network          Nexthop       Metric   Localprf          Path

Route Distinguisher : 100:2

*>i 192.168.0.1/32  192.168.0.2      0      100    10 ?

*>i 192.168.1.0/32  192.168.0.2    0      100     ?

Route Distinguisher : 100:30

*>i 192.168.0.1/32  192.168.0.2      0      100    10 ?

*> 192.168.4.0  192.168.4.1         0            20 ?

* 192.168.4.0    0.0.0.0            0      32768     ?
```

***:** This route is valid.

s: This route is suppressed by the aggregate route.

S: This route is an old entry.

>: This route is optimized.

i: This route is learned from IBGP.

Nexthop: The next-hop route information.

Metric: The metric value of this route.

Localprf: The local priority attribute of this route.

Path: The AS-path included in this route.

i: The ORINGIN attribute of this route is IGP.

e: The ORINGIN attribute of this route is EGP.

?: The ORINGIN attribute of this route is the one other than IGP and EGP.

```
DES-7200# show bgp vpnv4 unicast vrf vpn1 summary

BGP router identifier 192.168.0.4 , local AS num 100

BGP  VRF vrf1 Route  Distinguisher : 100 : 30

BGP table version is 1

3 BGP AS-PATH entries

0 BGP community entries

Neibhbor   V   AS   MsgRcvd Msgsend  TblVer  IntQ

OutQ   Up/Down  State/PfxRcd

192.168.4.1 4  20    15      16    1       0    0

00:10:36 3

Total number of neighbors 1
```

Field	Description
num BGP AS-PATH entries	Number of BGP AS-Path entries
num BGP community entries	Number of BGP community entries
V	BGP version
AS	AS number of the BGP peer
MsgRcvd	Total BGP messages received from the BGP peer
Msgsend	Total BGP messages sent to the BGP peer
TblVer	Routing table version of the BGP VPN address family. The routing table will be updated once after sending all the VPN routes to the BGP peer.
Up/Down	Duration of the BGP peer or “never”, indicaing that the BGP peer is not set up
State/PfxRcd	Number of VPN routes received from the BGP peer or the state of the BGP peer

2.2.3 show ip extcommunity-list

Use this command to show the configuration of the extended community list.

show ip extcommunity-list [*extcommunity-list-num*| *extcommunity-list-name*]

Parameter description

Parameter	Description
extcommunity-list-num	Identifies standard or extended extcommunity list in the range of 1 to 199.
extcommunity-list-name	Name of standard or extended extcommunity list

Command mode

Privileged mode

Examples

```
DES-7200 # show ip extcommunity-list
Standard extended community-list 1
    10 permit RT:1:200
    20 permit RT:1:100
Standard extended community-list 2
    10 permit RT:1:200
Expanded extended community-list rt_filter
    13 permit 1:100
```

Related commands

Command	Description
ip extcommunity-list	Create the extended community list.
match extcommunity	Match the extended community list.
set extcommunity	Set the extended community list.

2.2.4 show ip ospf sham-links

Use this command to display the OSPF sham-link information.

show ip ospf *[process-id]* **sham-links [area** *area-id***]**

Parameter description

Parameter	Description
process-id	OSPF process-id
area *area-id*	The OSPF area-id of the sham-link can be a decimal integer ranging from 0 to 4294967295 or an IP address.

Default configuration

No

Command mode

Privileged user mode

Usage guidelines

This command is used to display the sham-link information of the OSPF instance.

Examples

```
DES-7200#show ip ospf sham-links

Sham Link SLINK1 to address 8.8.8.8 is up

  Area 0.0.0.0 source address 7.7.7.7, Cost: 10

  Output interface is GigabitEthernet 0/8

  Nexthop address 192.168.1.2

  Transmit Delay is 1 sec, State Point-To-Point,

  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5

    Hello due in 00:00:07

    Adjacency state Full
```

Related commands

Command	Description
-	-

2.2.5 show ip route vrf

Use this command to show the routing table entry of the VRF

show ip route vrf *vrf-name* [*ip-address mask* | **bgp | connected | isis | ospf | rip | static**]

Parameter description

Parameter	Description
vrf-name	VRF name
ip-address mask	Show the entry of the prefix of the specified route.
bgp	Show the route entry generated from BGP.
connected	Show the entry of directly-connected route.
isis	Show the route entry generated from ISIS.
ospf	Show the route entry generated from OSPF.
rip	Show the route entry generated from RIP.
static	Show the static route entry.

Command mode

Privileged mode

Examples

```
DES-7200# show ip route vrf vrf1
Codes: C - connected, S - static, R - RIP,B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2 ,
ia - IS-IS inter area
* - candidate default

B   192.168.0.1/32 , [200/0] via 192.168.0.2, 01:02:33
```

```
B   192.168.0.3/32 , [200/0] via 192.168.4.1 , 01:02:33
C   192.168.4.0/24 is directly connected ,eth1
```

Related commands

Command	Description
show ip vrf	Show the vrf configuration information

2.2.6 show ip vrf

Use this command to show the configured VRF information.

show ip vrf [*vrf-name*]

Parameter description

Parameter	Description
vrf-name	VRF name.

Command mode

Privileged mode

Usage guidelines

When the inputted parameter carries the VRF name, the command shows the VRF information. If no VRF name is specified, it shows the information of all VRFs.

Examples

```
DES-7200# show ip vrf vrf1
VRF pe1; default RD : 100:2
Interfaces:
Eth0
Export VPN route-target communities:
RT :100:30
No import VPN route-target community
No import route-map
```

Related

Command	Description

commands	**ip vrf**	Create a VRF instance
	rd	Configure the RD value
	route-target	Configure the RT value
	ip vrf forwarding	Bind the VRF with an interface

2.2.7 show vrf

Use this command to view the brief information of a VRF, which can be a single-protocol IPv4 VRF or a multi-protocol VRF:

show vrf [brief] [*vrf-name*]

Use this command to view the brief information of a VRF configured with an IPv4 address family, which can be a single-protocol IPv4 VRF:

show vrf ipv4 [*vrf-name*]

Use this command to view the brief information of a VRF configured with an IPv6 address family:

show vrf ipv6 [*vrf-name*]

Use this command to view the detailed information of a VRF, which can be a single-protocol IPv4 VRF or a multi-protocol VRF:

show vrf detail [*vrf-name*]

Parameter description

Parameter	Description
vrf-name	VRF name

Default configuration None

Command mode Privileged user mode

Usage guidelines None

Examples

Show the brief information of all VRFs.

```
DES-7200#show vrf
  Name       Default RD          Protocols   Interfaces
  aaa        <not set>           ipv4
  aab        <not set>
  bbb        <not set>           ipv6
  ccc        <not set>           ipv4,ipv6   Vl1
```

Related commands

Command	Description
ip vrf	Define a single-protocol IPv4 VRF
vrf definition	Define a multi-protocol VRF

DES-7200

Security Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

Network engineers

Technical salespersons

Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 AAA Configuration Commands

1.1 ID Authentication Related Command

1.1.1 aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list. The no form of this command is used to delete the 802.1x user authentication method list.

aaa authentication dot1x {**default** | *list-name*} method1 [*method2*...]

no aaa authentication dot1x {**default** | *list*-name}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.
list-name	Name of the 802.1x user authentication method list, which could be any character string.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS server group is supported.

Default N/A

Command mode	Global configuration mode.
Usage guidelines	If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use **aaa authentication dot1x** to configure a default or optional method list for 802.1x user authentication. The next method can be used for authentication only when the current method does not work.
Examples	The following example defines an AAA authentication method list named **RDS_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. `DES-7200(config)# aaa authentication dot1x rds_d1x group radius local`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
dot1x authentication	Associate a specific method list with the 802.1x user.
username	Define a local user database.

1.1.2 aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list. The **no** form of this command is used to delete the user authentication method list.

aaa authentication enable {**default** | *list-name*} method1 [*method2*...]

no aaa authentication enable default

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
method	It must be one of the keywords listed in the following

table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.

Default N/A

Command mode Global configuration mode.

Usage guidelines

If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable authentication negotiation. You must use **aaa authentication enable** to configure a default or optional method list for Enable authentication.

The next method can be used for authentication only when the current method does not work.

The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

Examples

The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
DES-7200(config)# aaa authentication enable default
group radius local
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
enable	Switchover the user level.
username	Define a local user database.

1.1.3 aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list. The **no** form of this command is used to delete the authentication method list.

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
list-name	Name of the user authentication method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.

Default N/A.

Command mode Global configuration mode.

Usage guidelines

If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use **aaa authentication login** to configure a default or optional method list for Login authentication.

The next method can be used for authentication only when the current method does not work.

You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

Examples

The following example defines an AAA Login authentication method list named **list-1**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
DES-7200(config)# aaa authentication login list-1 group radius local
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
login authentication	Apply the Login authentication method to the terminal lines.
username	Define a local user database.

1.1.4 aaa authentication ppp

Use this command to enable AAA PPP user authentication and configure the PPP user authentication method list. The **no** form of this command is used to delete the authentication method list.

aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication ppp {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.
list-name	Name of the user authentication method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS server group is supported.

Default	N/A
Command mode	Global configuration mode.
Usage guidelines	If the AAA PPP security service is enabled on the device, users must use AAA for PPP authentication negotiation. You must use **aaa authentication ppp** to configure a default or optional method list for PPP user authentication. The next method can be used for authentication only when the current method does not work.
Examples	The following example defines an AAA PPP authentication method list named **rds_ppp**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. `DES-7200(config)# aaa authentication ppp rds_ppp group radius local`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
ppp authentication	Associate a specific method list with the PPP user.
username	Define a local user database.

1.1.5 login authentication

Use this command to apply the Login authentication method list to the specified terminal lines. The **no** form of this command is used to remove the application of Login authentication method list.

login authentication {**default** | *list-name*}

no login authentication

Parameter description

Parameter	Description
default	Apply the default Login authentication method list to the terminal line.
list-name	Apply the defined Login authentication method list to the terminal line.

Default	N/A
Command mode	Line configuration mode.
Usage guidelines	Once the default login authentication method list has been configured, it will be applied to all the terminals automatically. If non-default login authentication method list has been applied to the terminal, it will replace the default one. If you attempt to apply the undefined method list, it will prompt a warning message that the login authentication in this line is ineffective till it is defined.

Examples	The following example defines an AAA Login authentication method list named **list-1**. In the authentication method list, first the local user database is used for authentication. Then apply this method to VTY 0-4.
	`DES-7200(config)# aaa authentication login list-1 local`
	`DES-7200(config)# line vty 0 4`
	`DES-7200(config-line)# login authentication list-1`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
login authentication	Configure the Login authentication method list.
username	Define a local user database.

1.2 Authorization Related Commands

At present, DES-7200 supports authorization to the network protocols.

1.2.1 aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI. The **no** form of this command is used to disable the aaa authorization command function.

aaa authorization commands *level* {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization commands *level* {**default** | *list-name*}

Parameter description

Parameter	Description
level	Command level to be authorized, 0-15.
default	When this parameter is used, the following defined method list is used as the default method for command authorization.
list-name	Name of the user authorization method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform authorization.
group	Use the server group for authorization. At present, the RADIUS server group is supported.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

DES-7200 supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny.

It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.

The configured command authorization method must be applied to terminal line which requires for the command authorization. Otherwise, the configured command authorization method is ineffective.

Examples

The following example uses the TACACS+ server to authorize the level 15 command:

	`DES-7200(config)# aaa authorization commands 15 default group tacacs+`

Related commands	**Command**	**Description**
	aaa new-model	Enable the AAA security service.
	authorization commands	Apply the command authorization for to the terminal line.

1.2.2 aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode). The **no** form of this command is used to disable the configuration command authorization function.

aaa authorization config-commands

no aaa authorization config-commands

Parameter description	N/A
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.
Examples	The following example enables the configuration command authorization function: `DES-7200(config)# aaa authorization config-commands`

Related commands	**Command**	**Description**
	aaa new-model	Enable the AAA security service.

	aaa authorization commands	Define the AAA command authorization.

1.2.3 aaa authorization console

Use this command to authorize the commands of the users who has logged in the console. The **no** form of this command is used to disable the authorization function.

aaa authorization console

no aaa authorization console

Parameter description	N/A
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	DES-7200 supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.
Examples	The following example enables the aaa authorization console function: `DES-7200(config)# aaa authorization console`

Related commands	**Command**	**Description**
	aaa new-model	Enable the AAA security service.
	aaa authorization commands	Define the AAA command authorization.
	authorization commands	Apply the command authorization to the terminal line..

1.2.4 aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level. The **no** form of this command is used to disable the aaa authorization exec function.

aaa authorization exec {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization exec {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
list-name	Name of the user authorization method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authorization.
none	Do not perform authorization.
group	Use the server group for authorization. At present, the RADIUS server group is supported.

Default Disabled.

Command mode Global configuration mode.

Usage guidelines

DES-7200 supports authorization of users logged in the NAS CLI and assignment of CLI authority level(0-15). The aaa authorization exec function is effective on condition that Login authentication function has been enabled. It can not enter the CLI if it fails to enable the aaa authorization exec.

You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

Examples The following example uses the RADIUS server to

authorize Exec:

```
DES-7200(config)# aaa authorization exec default group
radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
authorization exec	Apply the command authorization to the terminal line .
username	Define a local user database.

1.2.5 aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network. The **no** form of this command is used to disable the authorization function.

aaa authorization network {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization network {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform authorization.
group	Use the server group for authorization. At present, the RADIUS server group is supported.

Default Disabled.

Command mode Global configuration mode.

Usage guidelines DES-7200 supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or

	interfaces will be authorized automatically. Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used. The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

Examples	The following example uses the RADIUS server to authorize network services: `DES-7200(config)# aaa authorization network default group radius`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accounting	Define AAA accounting .
aaa authentication	Define AAA authentication.
username	Define a local user database.

1.2.6 authorization commands

Use this command to apply the list of command authorization to the specific terminal line in the line configuration mode. The **no** form of this command is used to disable this function.

authorization commands *level* {**default** | *list-name*}

no authorization commands *level*

Parameter description

Parameter	Description
level	The authorized command level, 0-15.
default	Use the default command authorization command.
list-name	Apply a defined method list of the command authorization.

Default	Disabled.

Command mode	Line configuration mode.
Usage guidelines	Once the default command authorization method list has been configured, it is applied to all terminals automatically. Once the non-default command authorization method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the command authorization in this line is ineffective tilll the authorization method list is defined.

Examples	The following example configures the command authorization method list with name cmd, authorizes command level 15, uses the TACACS+ server. If the security server does not response, it does not perform authorization. After configuration, the authorization command is applied to VTY 0-4 lines:
	`DES-7200(config)# aaa authorization commands 15 cmd group tacacs+ none`
	`DES-7200(config)# line vty 0 4`
	`DES-7200(config-line)# authorization commands 15 cmd`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the method list of the AAA command authorization.

1.2.7 aaa authorization exec

Use this command to apply the Exec authorization methos list to the specified terminal lines in the line configuration mode. The **no** form of this command is used to disable the authorization function.

authorization exec {**default** | *list-name*}

no authorization exec

Parameter description

Parameter	Description
default	Use the default method of Exec authorization.
list-name	Apply a defined method list of Exec authorization.

Default

Disabled.

Command mode

Line configuration mode.

Usage guidelines

Once the default execauthorization method list has been configured, it is applied to all terminals automatically. Once the non-default command authorization method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the exec authorization in this line is ineffective tilll the authorization method list is defined.

Examples

The following example configures the exec authorization method list with name exec-1, uses the RADIUS server. If the security server does not response, it does not perform authorization. After configuration, the authorization command is applied to VTY 0-4 lines:

```
DES-7200(config)# aaa authorization exec exec-1 group radius none

DES-7200(config)# line vty 0 4

DES-7200(config-line)# authorization exec exec-1
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the method list of AAA Exec authorization.

1.3 Accounting Related commands

At present, DES-7200 supports network accounting using RADIUS.

1.3.1 aaa accounting commands

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting commands *level* {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting commands *level* {**default** | *list-name*}

Parameter description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.
default	When this parameter is used, the following defined method list is used as the default method for command accouting.
list-name	Name of the command accouting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform accouting.
group	Use the server group for acouting, the TACACS+ server group is supported.

Default Disabled.

Command mode Global configuration mode.

Usage guidelines

DES-7200 enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.

The configured accounting command method must be applied to the terminal line that needs accounting

command; otherwise it is ineffective.

Examples

The following example performs accounting of the network service requests from users using TACACS+, and configures the accounting command level to 15:

```
DES-7200(config)# aaa accounting commands 15 default start-stop group tacacs+
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the accouting commands to the terminal line.

1.3.2 aaa accounting exec

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting exec {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting exec {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec accouting.
list-name	Name of the Exec accouting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform accouting.
group	Use the server group for acouting, the RADIUS and TACACS+ server group is supported.

Default Disabled.

Command mode	Global configuration mode.
Usage guidelines	DES-7200 enables the exec accounting function after enabling the login authentication. After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user loggs in, it does not send the account stop information to the security server when a user loggs out, either. The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.
Examples	The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access: `DES-7200(config)# aaa accounting network start-stop group radius`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the Exec accouting to the terminal line..

1.3.3 aaa accounting network

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting network {**default** | *list-name*} **start-stop group radius**

no aaa accounting network {**default** | *list-name*}

Parameter description

Parameter	Description
network	Perform accounting of the network related service requests, including dot1x, PPP, etc.

resource	Perform accounting of resource related service requests.
list-name	Name of the accounting method list
start-stop	Send accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
group	Use the server group for accounting.
radius	Use the RADIUS group for accounting.

Default Disabled.

Command mode Global configuration mode.

Usage guidelines DES-7200 performs accounting of user activities by sending record attributes to the security server. Use the keyword **start-stop** to set the user accounting option.

Examples The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access:

```
DES-7200(config)# aaa accounting network start-stop
group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization network	Define a network authorization method list.
aaa authentication	Define AAA authentication.
username	Define a local user database.

1.3.4 aaa accounting update

Use this command to enable the accounting update function The **no** form of this command is used to disable the accounting update function.

aaa accounting update

no aaa accounting update

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.
Examples	The following example demonstrates how to enable the accounting update function. `DES-7200(config)# aaa new-model`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accounting network	Define a network accounting method list.

1.3.5 aaa accounting update periodic

If the accounting update function has been enabled, use this command to set the interval of sednign the accounting update message. The **no** form of this command is used to restore it to the default value.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter description

Parameter	Description
interval	Interval of sending the accounting update message, in minute. The shortest interval is 1 minute.

Default	5 minutes.
Command mode	Global configuration mode.
Usage guidelines	If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Examples	The following example demonstrates how to set the interval of accounting update to 1 minute.
	`DES-7200(config)# aaa new-model`
	`DES-7200(config)# aaa accounting update`
	`DES-7200(config)# aaa accounting update periodic 1`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accounting network	Define a network accounting method list.

1.3.6 accounting commands

Use this command to apply the accounting command list to the specified terminal lines. The **no** form of this command is used to disable the accounting function.

accounting commands *level* {**default** | *list-name*}

no accounting commands *level*

Parameter description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.
default	Use the default method of accouting commands.
list-name	Use a defined command accouting method list.

Default	Disabled.

Command mode	Line configuration mode.
Usage guidelines	Once the default command accouting method list has been configured, it is applied to all terminals automatically. Once the non-default command accounting method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the command authorization in this line is ineffective till the accounting command method list is defined.

Examples	The following example configures the accounting command method list with name cmd, accounts the level-15 command, uses the TACACS+ server. If the security server does not response, it does not perform accounting. After configuration, the accounting command is applied to VTY 0-4 lines:
	`DES-7200(config)# aaa accounting commands 15 cmd group tacacs+ none`
	`DES-7200(config)# line vty 0 4`
	`DES-7200(config-line)# accounting commands 15 cmd`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accouting commands	Define the method list of AAA accouting command.

1.3.7 accounting exec

Use this command to apply the exec accouting method list to the specified terminal lines in the line configuration mode. The **no** form of this command is used to disable the exec accounting function.

accounting exec {**default** | *list-name*}

no accounting exec

Parameter description

Parameter	Description
default	Use the default method of Exec accouting.

	list-name	Use a defined Exec accouting method list.

Default Disabled.

Command mode Line configuration mode.

Usage guidelines Once the default exec accouting method list has been configured, it is applied to all terminals automatically. Once the non-default exec accounting method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the exec accounting in this line is ineffective till the exec accounting command method list is defined.

Examples The following example configures the exec accounting method list with name exec-1, uses the RADIUS server. If the security server does not response, it does not perform accounting. After configuration, the exec accounting is applied to VTY 0-4 lines:

```
DES-7200(config)# aaa accounting exec exec-1 group radius
none

DES-7200(config)# line vty 0 4

DES-7200(config-line)# accounting exec exec-1
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accouting commands	Define the method list of AAA Exec accouting.

1.4 Domain-name-based AAA Service Related Command

At present, DES-7200 supports domain-name-based AAA service configuration.

1.4.1 aaa domain

Use this command to configure the domain attributes.The **no** form of this command is used to remove the setting.

aaa domain {**default** | *domain-name*}

no aaa domain {**default |** *domain-name*}

Parameter description

Parameter	Description
default	Use this parameter to configure the default domain.
domain-name	The name of the specified domain.

Default No domain is configured.

Command mode Global configuration mode.

Usage guidelines

Use this command to configure the domain-name–based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this domain name, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

Examples

The following example configures the domain name.

```
DES-7200(config)# aaa domain DES-7200.com
DES-7200(config-aaa-domain)#
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

1.4.2 aaa domain enable

Use this command to enable domain-name-based AAA service, which is disabled by default. The **no** form of this command is used to disable the service.

aaa domain enable

no aaa domain enable

Parameter description	N/A.
Default	disabled
Command mode	Global configuration mode.
Usage guidelines	To perform the domain-name-based AAA service configuration, enable this service.
Examples	The following example enables the domain-name-based AAA service. `DES-7200(config)# aaa domain enable`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
show aaa doamin	Show the domain configuration.

1.4.3 access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users. The **no** form of this command is used to remove the setting.

access-limit *num*

no access-limit

Parameter description

Parameter	Description
num	The number used for the user limitation is only valid for the IEEE802.1 users.

Default	By default, no number of users is limited.
Command mode	Domain configuration mode.
Usage guidelines	This command limits the number of users for the domain.

Examples	The following example sets the number of users as 20 for the domain named DES-7200.com.
	`DES-7200(config)# aaa domain DES-7200.com`
	`DES-7200(config-aaa-domain)# access-limit 20`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
enable	Switchover the user level.
username	Define a local user database.

1.4.4 accounting network

Use this command to configure the Network accounting list. The **no** form of this command is used to remove the setting.

accounting network {**default** | *list-name*}

no accounting network

Parameter description

Parameter	Description
default	Use this parameter to specify the default method list.
list-name	The name of the network accounting list.

Default	With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.
Command mode	Domain configuration mode.

Usage guidelines	Use this command to configure the Network accounting method list for the specified domain.

Examples

The following example sets the Network accounting method list for the specified domain.

```
DES-7200(config)# aaa domain DES-7200.com
DES-7200(config-aaa-domain)# accounting network default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

1.4.5 authentication dot1x

Use this command to configure the IEEE802.1x authentication list. The **no** form of this command is used to remove the setting.

authentication dot1x {**default** | *list-name*}

no authentication dot1x

Parameter description

Parameter	Description
default	Use this parameter to specify the default method list
list-name	The name of the specified method list

Default	With no method list specified, if users send the request, the device will attempt to specify the default method list for users.
Command mode	Domain configuration mode.
Usage guidelines	Specify an IEEE802.1x authentication method list for the domain.
Examples	The following example sets an IEEE802.1x authentication

method list for the specified domain.

```
DES-7200(config)# aaa domain DES-7200.com
DES-7200(config-aaa-domain)# authentication dot1x
default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

1.4.6 authorization network

Use this command to configure the Network authorization list. The **no** form of this command is used to remove the setting.

authorization network {**default** | *list-name*}

no authorization network

Parameter description

Parameter	Description
default	Use this parameter to specify the default method list
list-name	The name of the specified method list.

Default

With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command mode

Domain configuration mode.

Usage guidelines

Specify an authorization method list for the domain.

Examples

The following example sets an authorization method list for the specified domain.

```
DES-7200(config)# aaa domain DES-7200.com
DES-7200(config-aaa-domain)# authorization network
default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

1.4.7 show aaa domain

Use this command to show all current domain information

show aaa domain [**default** | *domain-name*]

Parameter description

Parameter	Description
default	Use this parameter to show the default domain.
domain-name	Show the specified domain.

Default N/A

Command mode Privileged EXEC mode.

Usage guidelines If no domain-name is specified, all domain information will be displayed.

Examples The following example shows the domain named domain.com

```
DES-7200(config)# show aaa domain domain.com
=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
```

Related commands	Command	Description
	aaa new-model	Enable the AAA security service.
	aaa domain enable	Enable the domain-name-based AAA service.

1.4.8 state

Use this command to set whether the configured domain is valid. The **no** form of this command restore it to the default setting.

state {**block | active**}

no state

Parameter description	Parameter	Description
	block	The configured domain is invalid.
	active	The configured domain is valid.

Default	Active
Command mode	Domain configuration mode.
Usage guidelines	Use this command to set whether the specified configured domain is valid.

Examples	The following example set the configured domain to be invalid
	`DES-7200(config)# aaa domain DES-7200.com`
	`DES-7200(config-aaa-domain)# state block`

Related commands	Command	Description
	aaa new-model	Enable the AAA security service.
	aaa domain enable	Enable the domain-name-based AAA service.
	show aaa domain enable	Show the domain configuration .

1.4.9 username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers. The **no** form of this command restores it to the default setting.

username-format {**without-domain**| **with-domain**}

no username-format

Parameter description

Parameter	Description
without-domain	Set the user name without the domain information.
with-domain	Set the user name with the domain information.

Default Without-domain

Command mode Domain configuration mode.

Usage guidelines Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Examples The following example sets the user name without the domain information.

```
DES-7200(config)# aaa domain DES-7200.com
DES-7200(config-aaa-domain)# username-domain without-domain
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

1.5 AAA Server Group Commands

1.5.1 aaa group server

Use this command to configure the AAA server group. The **no** form of this command is used to delete the server group.

aaa group server {**radius** | **tacacs+**} *name*

no aaa group server {**radius** | **tacacs+**} *name*

Parameter description

Parameter	Description
name	Name of the server group. It cannot be the keywords "**radius"** and "**tacacs+**".

Command mode

Global configuration mode.

Usage guidelines

This command is used to configure the AAA server group. Currently, the RADIUS and TACACS+ server groups are supported.

Examples

The following example configures an AAA server group.

```
DES-7200(config)# aaa group server radius ss
DES-7200(config-gs-radius)# end
DES-7200#show aaa group
Group-name:  ss
Group Type:  radius
Referred:   1
Server List:
```

Related commands

Command	Description
show aaa group	Show the AAA server group information.

1.5.2 ip vrf forwarding

Use this command to select the **vrf** for the AAA server group. The **no** form of this command removes the setting.

ip vrf forwarding *vrf_name*

no ip vrf forwarding

Parameter description

Parameter	Description
vrf_name	VRF name

Default Configuration N/A.

Command mode Server group configuration mode.

Usage guidelines This command selects VRF for the specified server groups.

Examples

The following example selects the VRF for the server group.

```
DES-7200(config)# aaa group server radius ss
DES-7200(config-gs-radius)# server 192.168.4.12
DES-7200(config-gs-radius)# server 192.168.4.13
DES-7200(config-gs-radius)# ip vrf forwarding vrf_name
DES-7200(config-gs-radius)# end
```

Related commands

Command	Description
aaa group server	Configure the AAA server group.
show aaa group	Show the AAA server group information.

1.5.3 server

Use this command to add a server to the AAA server group. The **no** form is used to delete a server.

server *ip-addr* [**authen-port** *port1*] [**acct-port** *port2*]

no server *ip-addr* [**authen-port** *port1*] [**acct-port** *port2*]

Parameter description

Parameter	Description
ip-addr	IP address of the server
port1	Authentication port of the server
port2	Accounting port of the server

Default	No server is configured.
Command mode	Server group configuration mode.
Usage guidelines	Add a server to the specified server group. The default value is used if no port is specified.

Examples	The following example adds a server to the server group.
	`DES-7200(config)# aaa group server radius ss`
	`DES-7200(config-gs-radius)# server 192.168.4.12 acct-port 5 authen-port 6`
	`DES-7200(config-gs-radius)# end`
	`DES-7200# show aaa group`
	`Group-name: ss`
	`Group Type: radius`
	`Referred: 2`
	`Server List:`
	`IP Address: 192.168.4.12`
	`Authentication Port: 6`
	`Accounting Port: 5`
	`Referred: 1`

Related commands

Command	Description
aaa group server	Configure the AAA server group.
show aaa group	Show the AAA server group information.

1.5.4 show aaa group

Use this command to show all the server groups configured for AAA.

show aaa group

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.

Usage guidelines	N/A.

Examples

The following example shows all the server groups configured for AAA.

```
DES-7200# show aaa group
Group Name:  ss
Group Type:  radius
Referred:    2
Server List:
IP Address: 192.168.217.64
Authentication Port: 1812
Accounting Port: 1813
Referred:  1
```

Related commands

Command	Description
aaa group server	Configure the AAA server group.

1.6 Other AAA Commands

1.6.1 aaa local authentication attempts

Use this command to configure login attempt times .

aaa local authentication attempts *max-attempts*

Parameter description	In the range of 1 to 2147483647.
Default	The default value is 3.
Command mode	Global configuration mode.
Usage guidelines	Use this command to configure login attempt times.
Examples	`DES-7200 #configure terminal`

	DES-7200 (config)#**aaa local authentication attempts** 6

Related commands	**Command**	**Description**
	show running-config	Show the current configuration of the switch.
	show aaa lockout	Show the lockout configuration parameter of current login.

1.6.2 aaa local authentication lockout-time

Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times .

aaa local authentication lockout-time *lockout-time*

Parameter description	In the range of 1 to 2147483647.
Default	15 hours.
Command mode	Global configuration mode.
Usage guidelines	Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times .
Examples	DES-7200#**configure terminal** DES-7200(config)#**aaa local authentication lockout-time** 5

Related commands	**Command**	**Description**
	show running-config	Show the current configuration of the switch.
	show aaa lockout	Show the lockout configuration parameter of current login.

1.6.3 aaa new-model

Use this command to enable the DES-7200 AAA security service. The **no** form of this command is used to disable the AAA security service.

aaa new-model

no aaa new-model

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.
Examples	The following example shows how to enable the AAA security service. `DES-7200(config)# aaa new-model`

Related commands

Command	Description
aaa authentication	Define a user authentication method list.
aaa authorization	Define a user authorization method list.
aaa accouting	Define a user accouting method list.

1.6.4 clear aaa local user lockout

Use this command to clear the lockout user list.

clear aaa local user lockout {all | user-name <*word*>**}**

Parameter description

Parameter	Description
word	User ID.

Default	N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to clear all the user lists or the specified user list.
Examples	`DES-7200(config)# clear aaa local user lockout all`

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

1.6.5 debug aaa

Use this command to turn on the AAA service debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug aaa event

no debug aaa event

Parameter description	N/A.
Command mode	Privileged EXEC mode.

1.6.6 show aaa method-list

Use this command to show all AAA method lists.

show aaa method-list

Parameter description	N/A.
Default	N/A.

Command mode	Privileged EXEC mode.

Usage guidelines	Use this command to show all AAA method lists.

Examples

The following example shows the AAA method list.

```
DES-7200# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local  group angel group
rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorizating network default group radius
```

Related commands

Command	Description
aaa authentication	Define a user authentication method list
aaa authorization	Define a user authorization method list
aaa accounting	Define a user accounting method list

1.6.7 show aaa user lockout

Use this command to show the lockout user list.

show aaa local user lockout {all | user-name <*word*>**}**

Parameter description

Parameter	Description
word	User ID.

Default	N/A.

Command mode	Privileged EXEC mode.

Usage guidelines

Use this command to show the lockout user list and show how long the lockout-time is.

Examples

```
DES-7200# show aaa user lockout all
```

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

2 RADIUS Configuration Commands

2.1 Configuration Related Commands

2.1.1 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packets. Use the **no** form of this command to delete the source IP address for the RADIUS packet.

ip radius source-interface *interface*

no radius source-interface

Parameter description

Parameter	Description
Interface	Interface that the source IP address of the RADIUS packet belongs to.

Default

The source IP address of the RADIUS packet is set by the network layer.

Command mode

Global configuration mode.

Usage guidelines

In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

Examples

The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface and uses it as the source IP address of the RADIUS packet:

	DES-7200(config)# **ip radius source-interface fastEthernet** *0/0*

Related commands	**Command**	**Description**
	radius-server host	Define the RADIUS server.
	ip address	Configure the IP address of the interface.

2.1.2 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute in the global configuration mode. Use the **no** form of this command to restore to the default value.

radius-server attribute 31 mac format {**ietf** | **normal** | **unformatted**}

no radius-server attribute 31 mac format

Parameter description	**Parameter**	**Description**
	ietf	The standard format specified by the IETF（RFC3580）. ‘-’ is used as the seperator, for example: 00-D0-F8-33-22-AC.
	normal	Normal format representing the MAC address. ‘.’ is used as the seperator. For example: 00d0.f833.22ac.
	unformatted	No format and seperator. By default, unformatted is used. For example: 00d0f83322ac.

Default	The default format is **unformatted**.
Command mode	Global configuration mode.
Usage guidelines	Some RADIUS security servers(mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

Examples	The following example shows how to define the RADIUS Calling-Station-ID attribute as IETF format: `DES-7200(config)# radius-server attribute 31 mac format ietf`

Related commands	**Command**	**Description**
	radius-server host	Define the RADIUS server.

2.1.3 radius-server host

Use this command to specify a RADIUS security server host. The **no** form of this command is used to delete the RADIUS security server host.

radius-server host { *ipv4-address* | *ipv6-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]]

no radius-server host { *ipv4-address* | *ipv6-address*}

Parameter description

Parameter	**Description**
hostname	DNS name of the RADIUS security server host.
ip-address	IP address of the RADIUS security server host.
auth-port	UDP port used for RADIUS authentication.
port-number	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
acct-port	UDP port used for RADIUS accounting.
port-number	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
test username *name*	(Optional) Enable the active detection to the RADIUS security server and specify the username used by the active detection.

idle-time *time*	(Optional) Set the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
ignore-auth-port	(Optional) Disable the detection to the authentication port on the RADIUS security server. It is enabled by default.
ignore-acct-port	(Optional) Disable the detection to the authentication port on the RADIUS security server. It is enabled by default.

Default No RADIUS host is specified.

Command mode Global configuration mode.

Usage guidelines In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

Examples

The following example defines a RADIUS security server host:

```
DES-7200(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
DES-7200(config)# radius-server host 192.168.100.1 test username viven idle-time 60 ignore-acct-port
```

The following example defines a RADIUS security server host in the IPv6 environment

```
DES-7200(config)# radius-server host 3000::100
```

Related commands

Command	Description
aaa authentication	Define the AAA authentication method list

	radius-server key	Define a shared password for the RADIUS security server.
	radius-server retransmit	Define the number of RADIUS packet retransmissions.
	radius-server timeout	Define the timeout for the RADIUS packet.

2.1.4 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server. The **no** form of this command is used to remove the shared password.

radius-server key [0 | 7] *text-string*

no radius-server key

Parameter description

Parameter	Description
text-string	Text of the shared password
0 | 7	Password encryption type. 0: no encryption; 7: Simply-encrypted.

Default No shared password is specified.

Command mode Global configuration mode.

Usage guidelines A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

Examples The following example defines the shared password **aaa** for the RADIUS security server:

```
DES-7200(config)# radius-server key aaa
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.

	radius-server retransmit	Define the number of RADIUS packet retransmissions.
	radius-server timeout	Define the timeout for the RADIUS packet.

2.1.5 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond. The **no** form of this command is used to restore it to the default setting.

radius-server retransmit *retries*

no radius-server retransmit

Parameter description

Parameter	Description
retries	Number of retransmissions

Default The default number of retransmissions is 3.

Command mode Global configuration mode.

Usage guidelines AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

Examples The following example sets the number of retransmissions to 4:

```
DES-7200(config)# radius-server retransmit 4
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the timeout for the RADIUS packet.

2.1.6 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet. The **no** format of this command is used to restore it to the default setting.

radius-server timeout *seconds*

no radius-server timeout

Parameter description

Parameter	Description
seconds	Timeout in the range 1 to1000 seconds.

Default 5 seconds.

Command mode Global configuration mode.

Usage guidelines Use this command to change the timeout of packet retransmission.

Examples The following example sets the timeout to 10 seconds:

```
DES-7200(config)# radius-server timeout 10
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of the RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.

2.1.7 radius-server dead-ctriteria

This global configuration command is used to configure criteria on a device to determine that the Radius server is unreachable. The **no** form of this command is used to restore the default value.

radius-server dead-criteria {**time** *seconds* [**tries** *number*] | **tries** *number*}

no radius-server dead-criteria {**time** *seconds* [**tries** *number*] | **tries** *number*}

Parameter description

Parameter	Description
time *seconds*	Configure the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range of 1s to 120s.
tries *number*	Configure the successive timeout times. When sending a request from the device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range of 1 to 100.

Default

time *seconds*: 60s.

tries *number*: 10.

Command mode

Global configuration mode.

Usage guidelines

If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

Examples

The following example sets the timeout to 120s and timeout times to 20.

```
DES-7200(config)# radius-server dead-criteria time 120 tries 20
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server deadtime	Define the duration when a device stops sending any requests to an unreachable Radius server.
radius-server timeout	Define the timeout for the packet retransmission.

2.1.8 radius-server deadtime

The global configuration command is used to configure the duration when a device stops sending any requests to an unreachable Radius server. The **no** form of this command is used to recover the default value.

radius-server deadtime *minnutes*

no radius-server deadtime

Parameter description

Parameter	Description
minutes	Define the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range of 1 min to 1440 min (24h).

Default

The default value of minutes is 0 min, that is, the device keeps sending requests to the unreachable Radius server.

Command mode

Global configuration mode.

Usage guidelines

If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorted than the unreachable time..

Examples

The following example sets the duration when the device stops sending requests to 1 min.

```
DES-7200(config)# radius-server deadtime 1
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server dead-criteria	Define the criteria to determine that a Radius server is unreachable.

2.1.9 radius attribute

radius attribute {*id* **| down-rate-limit | dscp | mac-limit | up-rate-limit**} **vendor-type** *type*

no radius attribute {*id* **|down-rate-limit | dscp | mac-limit | up-rate-limit**} **vendor-type**

Parameter description

Parameter	Description
id	Function ID in the range 1 to 255
type	Private attribute type

Default

Only the default configuration of private attributes in DES-7200 is recognized.

id	Function	Type
1	max down-rate	1
2	qos	2
3	user ip	3
4	vlan-id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42

Extended attributes:

id	Function	Type

1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan-id.	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Command mode

Global configuration mode.

Usage guidelines

Use this command to configure the type value of a private attribute.

Examples

The following example sets the type of max up-rate to 211:

```
DES-7200(config)# radius attribute 16 vendor-type 211
```

Related

Command	Description

commands	**radius set qos cos**	Set the qos value sent by the RADIUS server as the cos value of the interface.

2.1.10 radius set qos cos

Use this command to set the qos value sent by the RADIUS server as the cos value of the interface. Use the **no** form of this command to restore it to the default setting.

radius set qos cos

no radius set qos cos

Parameter description	N/A.
Default	Set the qos value sent by the RADIUS server as the dscp value.
Command mode	Global configuration mode.
Usage guidelines	Set the qos value sent by the RADIUS server as the cos value, and the dscp value by default.
Examples	The following example sets the qos value sent by the RADIUS server as the cos value of the interface.: `DES-7200(config)# radius set qos cos`

Related commands	**Command**	**Description**
	radius vendor-specific extend	Extend RADIUS not to differentiate the IDs of private vendors.

2.1.11 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors. Use the **no** form of this command to disable the function.

radius vendor-specific extend

no radius vendor-specific extend

Parameter description	N/A.
Default	Only the private vendor IDs of DES-7200 are recognized.
Command mode	Global configuration mode.
Usage guidelines	Use this command to identify the attributes of all vendor IDs by type.
Examples	The following example extends RADIUS not to differentiate the IDs of private vendors: `DES-7200(config)# radius vendor-specific extend`

Related commands

Command	Description
radius attribute	Configure vendor type.
radius set qos cos	Set the qos value sent by the RADIUS server as the cos value of the interface.

2.2 Showing Related Commands

2.2.1 debug radius

Use this command to turn on the RADIUS debugging switch. The **no** form of this command is used to turn off the RADIUS debugging switch.

debug radius {**event | detail**}

no debug radius {**event | detail**}

Parameter Description	N/A.
Command mode	Privileged EXEC configuration mode.

2.2.2 show radius server

Use this command to show the configuration of the RADIUS server.

show radius server

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples

```
DES-7200# show radius server
erver IP:   192.168.4.12
Accounting  Port:  23
Authen  Port:    77
Test Username:    viven
Test Idle Time:   10 Minutes
Test Ports:       Authen
Server State:    Active
   Current duration 765s, previous duration 0s
   Dead: total time 0s, count 0
   Statistics:
      Authen: request 15, timeouts 1
      Author: request 0, timeouts 0
      Account: request 0, timeouts 0

Server IP:   192.168.4.13
Accounting Port:  45
Authen  Port:    74
Test Username:    <Not Configured>
Test Idle Time:   60 Minutes
Test Ports:       Authen and Accounting
Server State:    Active
   Current duration 765s, previous duration 0s
```

```
    Dead: total time 0s, count 0
    Statistics:
        Authen: request 0, timeouts 0
        Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the packet transmission timeout.

2.2.3 show radius parameter

Use this command to show the global parameters of the RADIUS server.

show radius parameter

Parameter description N/A.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples

```
DES-7200# show radius parameter
Server Timout:    5 Seconds
Server Deadtime:  0 Minute
Server Retries:   3
Server Dead Critera:
    Time:       10 Seconds
    Tries:      10
```

Related commands	Command	Description
	radius-server host	Define the RADIUS security server.
	radius-server retransmit	Define the number of RADIUS packet retransmissions.
	radius-server key	Define a shared password for the RADIUS server.
	radius-server timeout	Define the packet transmission timeout.

2.2.4 show radius vendor-specific

Use this command to show the configuration of the private vendors.

show radius vendor-specific

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples

```
DES-7200#show radius vendor-specific
id    vendor-specific     type-value
----- -------------------- ----------
1     max-down-rate       1
2     port-priority       2
3     user-ip             3
4     vlan-id             4
5     last-supplicant-vers 5
      ion
6     net-ip              6
7     user-name           7
8     password            8
```

```
9    file-directory      9
10   file-count          10
11   file-name-0         11
12   file-name-1         12
13   file-name-2         13
14   file-name-3         14
15   file-name-4         15
16   max-up-rate         16
17   current-supplicant-v 17
     ersion
18   flux-max-high32     18
19   flux-max-low32      19
20   proxy-avoid         20
21   dialup-avoid        21
22   ip-privilege        22
23   login-privilege     42
26   ipv6-multicast-addre 79
     ss
27   ipv4-multicast-addre 87
     ss
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the packet transmission timeout.

3 TACACS+ Configuration Commands

3.1 Related Commands of TACACS+ Configuration

3.1.1 aaa group server tacacs+

Use this command to configure TACACS+ group server, dividing different TACACS+ servers to the different groups.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Parameter description

Parameter	Description
group_name	TACACS+ server group name

Default Configuration

No TACACS+ server group is configured.

Command mode

Global configuration mode.

Usage guidelines

By dividing TACACS+ servers into several groups, the tasks of anthentication, authorization and accounting can be implemented by different server groups.

Examples

The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group:

```
DES-7200(config)#aaa group server tacacs+ tac1
DES-7200(config-gs-tacacs+)# server 1.1.1.1
DES-7200(config-gs-tacacs+)# ip vrf forwarding vpn1
```

Related commands	Command	Description
	server	Configure server list of TACACS+ server group.
	ip vrf forwarding	Configure VRF name supported by TACACS+ server group.

3.1.2 server(TACACS+)

Use this command to configure server address in TACACS+ group server.

server *ip-address*

no server *ip-address*

Parameter description	Parameter	Description
	ip-address	server address in TACACS+ group server

Default Configuration	N/A

Command mode	TACACS+ group server configuration mode.

Usage guidelines	You must enter TACACS+ server group configuration mode to configure this command. To configure server address in TACACS+ group server, you must execute **tacacs-server host** in the global configuration mode. For the server address in TACACS+ group servers, when one server does not reply, it will send the request to the next server.

Examples	The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group:
	`DES-7200(config)#aaa group server tacacs+ tac1`
	`DES-7200(config-gs-tacacs+)#server 1.1.1.1`

Related commands

Command	Description
aaa group server tacacs+	Configure TACACS+ server group.
ip vrf forwarding	Configure VRF name supported by TACACS+ server group.

3.1.3 ip vrf forwarding(TACACS+)

Use this command to configure vrf name used by TACACS+ group server (this command exists in the device supporting VRF)

ip vrf forwarding *vrf-name*

no ip vrf forwarding

Parameter description

Parameter	Description
vrf-name	VRF name.

Default Configuration

N/A

Command mode

TACACS+ group server configuration mode.

Usage guidelines

Specify vrf name to the specified TACACS+ server.

Examples

The following example specifies VRF name as vpn1 to TACACS+ server group:

```
DES-7200(config)# aaa group server tacacs+ tac1
DES-7200(config-gs-tacacs+)# server 1.1.1.1
DES-7200(config-gs-tacacs+)# ip vrf forwarding vpn1
```

Related

Command	Description

commands	**aaa group server tacacs+**	Configure TACACS+ server group.
	server	Configure server list of TACACS+ server group.

3.1.4 ip tacacs source-interface

Use this command to configure the source address of TACACS+ packet:

ip tacacs source-interface *interface*

no ip tacacs source-interface

Parameter description	**Parameter**	**Description**
	interface	Source address interface of TACACS+ packet

Default Configuration	The source address of TACACS+ packet is set on network layer.
Command mode	Global configuration mode.
Usage guidelines	To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to set the source address of TACACS+ packet. This command specifies the first ip address of the specified interface as the source address of TACACS+ packet and is used on L3 devices.
Examples	The following example specifies TACACS+ packet to obtain ip address from fastEthernet 0/0 as the source address of TACACS+ packet : `DES-7200(config)# ip tacacs source-interface fastEthernet 0/0`

Related commands	**Command**	**Description**
	tacacs-server	Define TACACS+ server.

host	
ip address	Configure ip address of the interface.

3.1.5 tacacs-server host

Use this command to configure IP address of TACACS+ server host:

tacacs-server host {*ip-address* | *ipv6-address*} [**port** *integer*] [**timout** *integer*] [**key** *string*]

no tacacs-server host {*ip-address* | *ipv6-address*}

Parameter description

Parameter	Description
ip-address	IP address of TACACS+ server host.
ipv6-address	IPv6 address of TACACS+ server host.
port *integer*	TCP port used in TACACS+ communication.
timeout *integer*	Timeout time of TACACS+ host.
key *string*	Shared keyword of TACACS+ client and server.

Default Configuration

No specified TACACS+ host.

Command mode

Global configuration mode.

Usage guidelines

To use TACACS+ to implement AAA security service, you must define TACACS+ secure server. You can define one or multiple TACACS+ secure servers by using **tacacs-server host.**

Examples

The following example defines a TACACS+ secure server host:

```
DES-7200(config)# tacacs-server host 192.168.12.1

DES-7200(config)# tacacs-server host 2001::1
```

Related commands

Command	Description
aaa authentication	Define AAA identity authentication method list.
tacacs-server key	Define the shared password of TACACS+ secure server globally.
tacacs-server timeout	Define timeout timer of reply packet of TACACS+ server globally.

3.1.6 tacacs-server key

Use this command to configure global password of TACACS+ :

tacacs-server key [*0* | *7*] *string*

no tacacs-server key

Parameter description

Parameter	Description
string	Text of shared password.
***0*	*7***	Encryption type of password, 0 indicates no encryption ; 7 indicates being simply encrypted.

Default Configuration No specified shared password.

Command mode Global configuration mode.

Usage guidelines The device and TACACS+ secure server communicates with each other successfully on the basis of the shared password. Therefore, in order to make the device and TACACS+ secure server communicate with each other, the same shared password must be defined on both of them. When we need to specify different passwords to every server, use key option in **tacacs-server host** command. We can set a key to all the servers that have not set key option in global configuration mode.

Examples The following example defines the shared password of TACACS+ secure server as aaa:

```
DES-7200(config)# tacacs-server key aaa
```

Related commands

Command	Description
tacacs-server host	Define TACACS+ secure server host.
tacacs-server timeout	Define the timeout timer of TACACS+ packet.

3.1.7 tacacs-server timeout

Use this command to configure the global timeout time waiting for the server when communicatin with TACACS+ server :

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter description

Parameter	Description
seconds	Timeout time (s) in the range 1 to 1000s.

Default Configuration

5s.

Command mode

Global configuration mode.

Usage guidelines

Use this command to adjust the timeout time of reply packet. When we need to specify different timeout time to every server, use timeout option in **tacacs-server host** command. We can set a timeout to all the servers that have not set timeout option in global configuration mode.

Examples

The following example shows how to define the timeout time as 10s:

```
DES-7200(config)# tacacs-server timeout 10
```

Related commands	**Command**	**Description**
	tacacs-server host	Define TACACS+ secure server host.
	tacacs-server key	Define the shared password of TACACS+.

3.2 TACACS+ Privileged Command

3.2.1 debug tacacs+

Use this command to turn on the TACACS+ debugging switch. The **no** form of this command turns off the TACACS+ debugging switch.

debug tacacs+

no debug tacacs+

Parameter description	N/A.

Command mode	Privileged mode.

3.2.2 show tacacs

Use this command to show the interoperation condition with each TACACS+ server.

show tacacs

Parameter description	N/A.

Default configuration	N/A.

Command mode	Privileged EXEC mode.

Usage guidelines

Use this command to show the interoperation condition with each TACACS+ server.

Examples

```
DES-7200# show tacacs
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Related commands

Command	Description
tacacs-server host	Define TACACS+ secure server host.

4 802.1X Configuration Commands

4.1 dot1x Active Authentication Command

4.1.1.1 dot1x auto-req

Use this command to configure 802.1X active authentication function in the global configuration command. The **no** form of this command disables the automatic authentication function.

[**no**] **dot1x auto-req**

Default	Enabled
Command mode	Global configuration mode.
Usage guidelines	This command is used to actively initiate 802.1x authentication on the device. Use the **show dot1x auto-req** command to view the setting of this function.

Examples	The following example sets the device to automatically initiate 802.1x authentication:
	`DES-7200# configure terminal`
	`DES-7200(config)# dot1x auto-req`
	`DES-7200(config)# end`
	`DES-7200(config)# show dot1x auto-req`
	`Auto-Req: Enabled`
	`User-Detect : Enabled`
	`Packet-Num : 0`
	`Req-Interval: 30 Second`

Related	Command	Description

commands	**show dot1x auto-req**	Show the automatic authentication request information.

4.1.2 dot1x auto-req packet-num

Use this command to set the number of authentication request messages that the device automatically sends. The **no** form is used to specify the default value.

dot1x auto-req packet-num *num*

no dot1x auto-req packet-num

	Parameter	**Description**
Parameter description	*num*	Number of authentication request messages that the device sends automatically.

Default	num = 0; namely the packets are sent continuously.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x auto-req** command to view the setting of this function.

Examples

The following example sets the device to automatically initiate 802.1x authentication continuously:

```
DES-7200# configure terminal
DES-7200(config)# dot1x auto-req packet-num 0
DES-7200(config)# end
DES-7200# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Second
```

	Command	**Description**
Related commands	**show dot1x auto-req**	Show the authentication request information.

4.1.3 dot1x auto-req req-interval

Use this command to set the interval of sending authentication request messages. The **no** form is used to specify the default value.

dot1x auto-req req-interval *interval*

no dot1x auto-req req-interval

Parameter description

Parameter	Description
interval	The time interval of actively sending authentication request messages by the device, in second.

Default 30 seconds.

Command mode Global configuration mode.

Usage guidelines Use the **show dot1x auto-req** command to view the setting of this function.

Examples

The following example sets the time interval of sending authentication request message to 60s:

```
DES-7200# configure terminal
DES-7200(config)# dot1x auto-req req-interval 60
DES-7200(config)# end
DES-7200# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 60 Second
```

Related commands

Command	Description
show dot1x auto-req	Show the authentication request information.

4.1.4 dot1x auto-req user-detect

Use this command to disable the device to send authentication request message after receiving the response. The **no** form is used to specify the default value.

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter description	N/A.
Default	Enabled.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x auto-req** command to view the setting of this function.

Examples	The following example sets the device to stop sending authentication request messages after the user gets on line:
	`DES-7200# configure terminal`
	`DES-7200(config)# dot1x auto-req user-detect`
	`DES-7200(config)# end`
	`DES-7200# show dot1x auto-req`
	`Auto-Req: Enabled`
	`User-Detect : Enabled`
	`Packet-Num : 0`
	`Req-Interval: 60 Second`

Related commands

Command	Description
show dot1x auto-req	Show the authentication request information.

4.2 dot1x Timeout Parameter Setting Commands

4.2.1 dot1x timeout quiet-period

Use this command to set the time (in seconds) for the device to wait before reauthentication after the authentication failure (for example, incorrect authentication password). Use the **no** form of the command to restore it tothe default setting.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameter description

Parameter	Description
seconds	Time (in seconds) for the device to wait before reauthentication after the authentication failure The range is from 0 to 65535, in seconds.

Default

10 seconds.

Command mode

Global configuration mode.

Usage guidelines

When authentication fails, the solicitator must wait for a period of time before reauthentication.

Examples

The following example sets the time for waiting re-authentication to 1000s:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout quiet-period 1000
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:          Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       3600 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.2.2 dot1x timeout re-authperiod

Use this command to set re-authentication interval when re-authentication is enabled. Use the

no form of the command to restore it to the default value.

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Parameter description

Parameter	Description
seconds	Period of authentication. The range is from 0 to 65535 seconds.

Default 3600 seconds.

Command mode Global configuration mode.

Usage guidelines Use **show dot1x** command to show the 802.1X configuration.

Examples

The following example sets the period of re-authentication to 1000s:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout re-authperiod 1000
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:          Enabled
Authentication mode     EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.2.3 dot1x timeout server-timeout

Use this command to set the authentication timeout between the device and the authentication server. Use the **no** form of the command to restore it to the default setting.

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameter description

Parameter	Description
seconds	Authentication timeout between the device and the authentication server. The range is 0 to 65535 seconds.

Default 5 seconds.

Command mode Global configuration mode.

Usage guidelines Use **show dot1x** command to show 802.1X configuration.

Examples

The following example sets the authentication timeout of the authentication server to 10s:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout server-timeout 10
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:         Enabled
Authentication mode:   EAP-MD5
Authed User Number:    0
Re-authen Enabled:     Disabled
Re-authen Period:      1000 sec
Quiet Timer Period:    1000 sec
Tx Timer Period:       3 sec
Supplicant Timeout:    3 sec
Server Timeout:        10 sec
Re-authen Max:         3 times
Maximum Request:       3 times
Client Oline Probe:    Disabled
Eapol Tag Enable:      Disabled
Authorization Mode:    Group Server
```

Related commands	Command	Description
	show dot1x	Show the information about 802.1x.

4.2.4 dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant. Use the **no** form of the command to restore it to the default setting.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameter description	Parameter	Description
	seconds	Authentication timeout between the device and the supplicant The range is from 0 to 65535 seconds.

Default	3 seconds.

Command mode	Global configuration mode.

Usage guidelines	Use **show dot1x** command to show 802.1X configuration.

Examples

The following example sets the authentication timeout between the device and the supplicant to 10s:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout supp-timeout 10
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:          Enabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
```

```
Eapol Tag Enable:      Disabled
Authorization Mode:    Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.2.5 dot1x timeout tx-period

Use this command to set the interval of transmitting packets after the maximum number of retransmission times is configured. Use the **no** form of the command to restore it to the default setting.

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameter description

Parameter	Description
seconds	Period of retransmission. The range is from 0 to 65535 seconds.

Default 3 seconds.

Command mode Global configuration mode.

Usage guidelines Use **show dot1x** command to show 802.1X configuration.

Examples

The following example sets the interval of retransmission to 10s:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout tx-period 10
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:       Enabled
Authentication mode: EAP-MD5
Authed User Number:  0
Re-authen Enabled:   Disabled
Re-authen Period:    1000 sec
Quiet Timer Period:  1000 sec
Tx Timer Period:     10 sec
Supplicant Timeout:  10 sec
Server Timeout:      10 sec
Re-authen Max:       3 times
```

```
Maximum Request:      3 times
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.3 dot1x Re-authentication Commands

4.3.1 dot1x re-authentication

Use this command to enable periodic re-authentication. Use the **no** form of the command to restore it to the the default setting.

[**no**] **dot1x re-authentication**

Parameter description

N/A.

Default

By default, it is not required to re-authenticate the supplicant periodically.

Command mode

Global configuration mode.

Usage guidelines

This command will reauthenticate the supplicant periodically after he passes the authentication. Use **show dot1x** command to show 802.1X configuration.

Examples

The following example enables the re-authentication function:

```
DES-7200# configure terminal
DES-7200(config)# dot1x re-authentication
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:        Enabled
Authentication mode:  EAP-MD5
Authed User Number:   0
Re-authen Enabled:    Enabled
Re-authen Period:     1000 sec
Quiet Timer Period:   1000 sec
```

```
Tx Timer Period:      10 sec
Supplicant Timeout:   10 sec
Server Timeout:       10 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.3.2 dot1x reauth-max

Use this command to set the maximum number of supplicant reauthentication. Use the **no** form of the command to restore it to the default value.

dot1x reauth-max *count*

no dot1x reauth-max

Parameter description

Parameter	Description
count	Maximum number of re-authentications

Default The default value is 3.

Command mode Global configuration mode.

Usage guidelines Use this command to specify the maximum number of supplicant reauthentications. Use **show dot1x** command to show 802.1X configuration.

Examples The following example sets the maximum number of re-authentications:

```
DES-7200# configure terminal
DES-7200(config)# dot1x reauth-max 5
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:          Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enable
Re-authen Period:       1000 sec
```

```
Quiet Timer Period:    1000 sec
Tx Timer Period:       10 sec
Supplicant Timeout:    10 sec
Server Timeout:        10 sec
Re-authen Max:         5 times
Maximum Request:       3 times
Client Oline Probe:    Disabled
Eapol Tag Enable:      Disabled
Authorization Mode:    Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.4 dot1x Detection Function Commands

4.4.1 dot1x probe-timer

Use this command to enable the probe timer on the client.

dot1x probe-timer{**interval** | **alive**}*interval*

no dot1x probe-timer

Parameter description

Parameter	Description
no	Restore the setting to the default value.
interval	Interval of sending the Hello message.
alive	Alive interval
interval	Timer value

Default

The default Hello interval is 20 seconds.
Default user alive interval is 250 seconds

Command mode

Global configuration mode.

Usage guidelines

Configure the alive detection timer for the client. You can use the **show dot1x** command to show the 802.1x setting.

Examples

The following example sets the Hello interval to 30 seconds and the alive interval to 120 seconds:

```
DES-7200# configure terminal
```

```
DES-7200(config)# dot1x probe-timer interval 30
DES-7200(config)# dot1x probe-timer alive 120
DES-7200(config)# end
DES-7200# show dot1x probe-timer
Hello Interval: 30 Seconds
Hello Alive: 120 Seconds
```

Related commands

Command	Description
Show dot1x probe-timer	Show the probe timer information.

4.4.2 dot1x client-probe enable

Use this command to enable the online probe function of the client

[**no**] **dot1x client-probe enable**

Parameter description

N/A.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

Use this command to enable the online probe function of the client.

Examples

Enable the online probe function of the client.

```
DES-7200# configure terminal
DES-7200(config)# dot1x client-probe enable
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:         Enabled
Authentication mode:   EAP-MD5
Authed User Number:    0
Re-authen Enabled:     Enabled
Re-authen Period:      1000 sec
Quiet Timer Period:    1000 sec
Tx Timer Period:       10 sec
Supplicant Timeout:    10 sec
Server Timeout:        10 sec
Re-authen Max:         5 times
Maximum Request:       3 times
```

```
Client Oline Probe:    Enabled
Eapol Tag Enable:      Disabled
Authorization Mode:    Group Server
```

Related commands

Command	Description
show dot1x	Show the 802.1x configurations.

4.5 Other dot1x Configuration Commands

4.5.1 dot1x authentication

In case the AAA is enabled, the authentication with the AAA server must be performed for logon. Use this command to associate logon authentication method list. The **no** form of this command is used to delete the logon authentication method list.

dot1x authentication {**default** | *list-name*}

no dot1x authentication {**default** | *list-name*}

Parameter description

Parameter	Description
default	Name of the default authentication method list
list-name	Name of the method list available

Default

If AAA is enabled, the AAA service is used for login authentication by default.

Command mode

Interface configuration mode.

Usage guidelines

If the AAA security server is enabled, this command is used for the login authentication with the specified method list.

Examples

The following command demonstrates how to associate a method list on the interface and use **group radius** for authentication.

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# aaa authentication dot1x default group
```

```
radius
DES-7200(config)# interface fastEthernet0/1
DES-7200(config-if)# dot1x authentication default
DES-7200(config-if)# end
DES-7200#
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication dot1x	Configure the logon authentication method list.

4.5.2 dot1x auth-address-table

Use this command to set the IP address list that 802.1X authentication allows. Use the **no** form of the command to remove the allowed IP address list.

dot1x auth-address-table address *mac-addr* **interface** *interface*

no dot1x auth-address-table address *mac-addr* **interface** *interface*

Parameter description

Parameter	Description
mac-addr	Physical IP address that can be authenticated.
interface	Interface number.

Default N/A.

Command mode Global configuration mode.

Usage guidelines Only the IP address in this list can be authenticated by 802.1X. Use **show dot1x auth-address table** command to show the authentication address list.

Examples The following example demonstrates how to add an authentication address on the interface.

```
DES-7200# configure terminal
DES-7200(config)# dot1x auth-address-table address
00d0f8000000 interface ehternet 1/1
DES-7200(config)# end
DES-7200#
```

	Command	Description
Related commands	**show dot1x auth-address-table**	Show the information about the IP address list that the 802.1x can authenticate.

4.5.3 dot1x auth-fail max-attempt

Use this command to set the maximum attempt times of entering the fail VLAN.

dot1x auth-fail max-attepmt *num*

no dot1x auth-fail max-attempt

	Parameter	Description
Parameter description	*num*	The maximum attempt times of entering the fail VLAN, ranging from 1 to 3.

Default	3
Command mode	Global configuration mode.
Usage guidelines	Use **show dot1x** command to show the configurations.

Examples	The following example demonstrates how to set the maximum attempt times of entering the fail VLAN.
	`DES-7200# configure terminal`
	`DES-7200(config)# dot1x auth-fail max-attempt 5`
	`DES-7200(config)# end`
	`DES-7200#`

	Command	Description
Related commands	**show dot1x**	Show the 802.1x configuration.

4.5.4 dot1x auth-fail vlan

Use this command to set the 802.1X authentication fail vlan.

dot1x auth-fail vlan *vid*

no dot1x auth-fail vlan *vid*

Parameter description

Parameter	Description
vid	Fail VLAN ID

Default No fail VLAN by default.

Command mode Interface configuration mode.

Usage guidelines Use **show dot1x interface** command to show the configurations.

Examples

The following example demonstrates how to set the 802.1X authentication fail vlan.

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x auth-fail vlan 2
DES-7200(config)# end
DES-7200#write
```

Related commands

Command	Description
show dot1x interface	Show the 802.1x configurations on the interface.

4.5.5 dot1x auth-mode

Use this command to specify the 802.1x authentication mode.

dot1x auth-mode {**eap-md5** | **chap** | **pap**}

no dot1x auth-mode

Parameter description

Parameter	Description
eap-md5	Use EAP-MD5 for authentication.
chap	Use CHAP for authentication.
pap	Use PAP for authentication.

Default EAP-MD5 mode.

Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x** command to show the 802.1X configurations.

Examples	This example shows how to configure the 802.1X authentication mode:
	`DES-7200# configure terminal`
	`DES-7200(config)# dot1x auth-mode chap`
	`DES-7200(config)# end`
	`DES-7200#`

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.5.6 dot1x critical

If all RADIUS authentication servers have no response and no other methods are configured in the effective 802.1x authentication method list, the user authentication fails and can not access the network by default. In this case, in order to guarantee the user accessing network, you can enable the server IAB(Inaccessible Authentication Bypass) on the port.

[**no**] **dot1x critical**

Parameter description

Parameter	Description
-	-

Default	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	With the IAB function enabled on the port, if there is only RADIUS authentication method in the 802.1x authentication method list and all RADIUS servers in this method list take no effect, the switch will set the network accessing authority for users by the IAB method, and send the EAPOL-SUCCESS packets to the users. Except for the RADIUS authentication method, if there are other authentication methods in the 802.1x authentication

method list, the IAB function will take no effect.(Such as the **aaa authentication dot1x default group radius none,** there exists the none authentication method after the RADIUS authentication method.

For the users of IAB authorized, as the user identity legality can not be checked, no matter whether the accounting function is configured, they will not send the accounting request.

With the AAA multi-domain authentication enabled globally, the 802.1x user authentication will not use the globally configured method list. After all RADIUS servers in the 802.1x globally configured method list are checked to be invalid, the IAB will directly send the successful authentication to the user with no need to enter the username, the AAA multi-domain authentication on this port is useless.

Examples

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
DES-7200(config)# interface fa 0/10
DES-7200(config-if)# dot1x port-control auto
DES-7200(config-if)# dot1x critical
DES-7200(config-if)# end
```

Related commands

Command	Description
-	-

4.5.7 dot1x critical recovery action reinitialize

Use this command to handle the all users that have passed the inaccessible authentication bypass on the port after the RADIUS server returns to normal. Use the **no** form of this command to restore it to the default settings.

[**no**] **dot1x critical recovery action reinitialize**

Parameter description

Parameter	Description
-	-

Default

By default, the server handles nothing after returning to normal.

Command mode	Interface configuration mode.
Usage guidelines	After the port entering the inaccessible authentication bypass status, if the RADIUS server returns to normal, you need to reinitialize the authentication for all users that have accomplished the network access authorization through the inaccessible authentication bypass on ports in order to ensure the user legality.
Examples	DES-7200# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. DES-7200(config)# **interface fa** *0/10* DES-7200(config-if)# **dot1x port-control auto** DES-7200(config-if)# **dot1x critical recovery action reinitialize** DES-7200(config-if)# **end**

Related commands

Command	Description
-	-

4.5.8 dot1x critical vlan

Use this command to configure the port in IAB status to jump to the specified fail-vlan. Use the **no** form of this command to disable this function.

dot1x critical vlan *vlan-id*

no dot1x critical vlan

Parameter description

Parameter	Description
vlan-id	The VLAN where the port will jump.

Default	Disabled.
Command mode	Interface configuration mode.

Usage guidelines	With this function enabled, if no user authentication is performed on the ports initially, after all RADIUS servers are invalidated, the user will initiate the authentication and the port will enter the IAB status and to be added to the VLAN configured. If this function is disabled, the VLAN of the port is not changed when the port is in the IAB status.
Examples	DES-7200# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. DES-7200(config)# **interface fa** *0/10* DES-7200(config-if)# **dot1x port-control auto** DES-7200(config-if)# **dot1x critical vlan** *100* DES-7200(config-if)# **end**

Related commands

Command	Description
-	-

4.5.9 dot1x default

Use this command to restore part of 802.1x parameters to the default value..

dot1x default

Parameter description	N/A.
Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x** command to show the 802.1X configuration.
Examples	The following example sets the default parameters of 802.1x: DES-7200# **configure terminal** DES-7200(config)# **dot1x default** DES-7200(config)# **end** DES-7200# **end**

Related commands	**Command**	**Description**
	show dot1x	Show the information about 802.1x.

4.5.10 dot1x dynamic-vlan enable

Use this command to enable dynamic VLAN. Use the **no** form of the command to disable the function.

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameter description	N/A.
Default	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	Use the **show dot1x dynamic-vlan** command to show the 802.1X configuration.

Examples	The following example enables dynamic VLAN:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface gigabitEthernet 4/5`
	`DES-7200(config-if)# dot1x dynamic-vlan enable`
	`DES-7200(config)# end`
	`DES-7200#`

Related commands	**Command**	**Description**
	show dot1x	Show the information about 802.1x.

4.5.11 dot1x guest-vlan

Use this command to set whether to allow **guest vlan** jump. Use the **no** form of the command to disable the function.

dot1x guest-vlan *vid*

no dot1x guest-vlan

Parameter description

Parameter	Description
vid	In the range from 1 to 4094.

Default Disabled.

Command mode Interface configuration mode.

Usage guidelines

1. Before using guest vlan, you need to execute **dot1x dynamic-vlan enable** command first，or the configured guest vlan does not take effect.

2. When configuring guest vlan, it is recommended not to modify L2 attribute of the port, especially not to add the port to a VLAN manually.

3. Execute **show running-config** to view 802.1x configuration.

Examples

The following example sets 802.1x guest vlan jumping:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 4/5
DES-7200(config-if)# dot1x guest-vlan 10
DES-7200(config)# end
DES-7200#
```

Related commands

Command	Description
show running-config	Show the configuration information about 802.1x.

4.5.12 dot1x eapol-tag

Use this command to tag the EAPOL frames. Use the **no** form of the command to disable the function.

dot1x eapol-tag

no dot1x eapol-tag

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x** command to show the 802.1X configuration.

Examples	The following example tags the EAPOL frames:
	`DES-7200# configure terminal`
	`DES-7200(config)# dot1x eapol-tag`
	`DES-7200(config)# end`
	`DES-7200#`

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.5.13 dot1x mac-auth-bypass

Use this command to set the 802.1x MAC bypass authentication.

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Parameter description	N/A.
Default	The 802.1x MAC bypass authentication is not supported by default.
Command mode	Interface configuration mode.
Usage guidelines	Use the **show dot1x port-control interface** command to show the configuration.
Examples	The following example sets the 802.1x MAC bypass

authentication:

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config)# dot1x mac-auth-bypass
DES-7200(config)# end
DES-7200#
```

Related commands

Command	Description
show dot1x port-control interface	Show the information about 802.1x on the interface .

4.5.14 dot1x mac-auth-bypass timeout-activity

Use this command to set the 802.1x MAC bypass authenticastion online time.

dot1x mac-auth-bypass timeout-activity *value*

no dot1x mac-auth-bypass timeout-activity

Parameter description

Parameter	Description
value	The online time, in seconds. The valid range is 1-65535.

Default No default value.

Command mode Interface configuration mode.

Usage guidelines Use the **show run** command to show the 802.1X configuration.

Examples

The following example sets the 802.1x MAC bypass authenticastion online time:

```
DES-7200# configure terminal
DES-7200(config)# interface fa0/1
DES-7200(config)# dot1x mac-auth-bypass
timeout-activity
DES-7200(config)# end
DES-7200#write
```

Related

Command	Description

commands	**show dot1x port-control interface**	Show the information about 802.1x on the interface.

4.5.15 dot1x mac-auth-bypass violation

Use this command to set the 802.1x MAC bypass authentication violation.

dot1x mac-auth-bypass violation

no dot1x mac-auth-bypass violation

Parameter description	N/A.
Default	No violation is processed by default.
Command mode	Interface configuration mode.
Usage guidelines	Use the **show run** command to show the 802.1X configuration.

Examples	The following example sets the 802.1x MAC bypass authentication violation:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface fa0/1`
	`DES-7200(config)# dot1x mac-auth-bypass violation`
	`DES-7200(config)# end`
	`DES-7200#write`

	Command	Description
Related commands	**show dot1x port-control interface**	Show the information about 802.1x on the interface.

4.5.16 dot1x max-req

During interaction between the dot1x and the server, the dot1x will send a request to the server again if it does not receive a response from the server within a certain period of time. Use this command to set the maximum number of authentication requests sent to the server. Use the **no** form of the command to restore it to the default value.

dot1x max-req *count*

no dot1x max-req

Parameter description

Parameter	Description
count	Maximum number of authentication requests sent to the server.

Default The default value is 3.

Command mode Global configuration mode.

Usage guidelines Use the **show dot1x** command to show the 802.1X configuration.

Examples The following example demonstrates how to set the maximum number of authentication requests to 7:

```
DES-7200# configure terminal
DES-7200(config)# dot1x max-req 7
DES-7200(config)# end
DES-7200#
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.5.17 dot1x private-supplicant-only

Use this command to support the private supplicant in the global configuration mode. The **no** form of this command restores it to the default value.

dot1x private-supplicant-only

no dot1x private-supplicant-only

Parameter description N/A.

Default configuration The private supplicant is supported.

Command mode	Global configuration mode.
Usage guidelines	You can use **show dot1x private-supplicant-only** to check the 802.1x setting.

Examples	Example
	This example configures to use the private supplicant only:
	`DES-7200# configure t`
	`DES-7200(config)# dot1x private-supplicant-only`
	`DES-7200(config)# end`
	`DES-7200#`

Related commands

Command	Function
show dot1x private-supplicant-only	Show the information about the private supplicant.

4.5.18 dot1x port-control auto

In the interface configuration mode, use this command to allow the port to participate in authentication. Use the **no** form of the command to restore it to the default value.

dot1x port-control auto

no dot1x port-control

Parameter description	N/A.
Default	By default, the port does not participate in 802.1x authentication.
Command mode	Interface configuration mode.

Usage guidelines	Use the **show dot1x** command to show the 802.1X configuration.

Examples

The following example sets the port to participate in authentication:

```
DES-7200# configure terminal
DES-7200(config)# interface g0/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config-if)# end
DES-7200#
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

4.5.19 dot1x port-control-mode

By default, 802.1x adopts MAC address-based control mode. In this mode, only authenticated users have access to the network, while other users that connect to the same port cannot access the network. In the port-based control mode, however, if one user that connects to the port passes the authentication, this port becomes an authenticated port and all the users that connect to this port have access to the network. In the port-based single-user control mode, the port is authenticated when it allows only one authenticated user who is enable to use the network normally. If you find other users on the port, you should clear all the users on the port and reauthenticate.The authentication mode can be configured using the following commands:

dot1x port-control-mode {**mac-based** | {**port-based [single-host]}**}

no dot1x port-control-mode

Parameter description

Parameter	Description
mac-based	Enable the MAC address-based control.
port-based	Enable port-based control.
single-host	Enable singlehost-based control.

Default	MAC address-based access control is used by default.
Command mode	Interface configuration mode.
Usage guidelines	Use the **show dot1x port-control** command to show the 802.1X configuration for the port.

Single-host is port-based single-user 802.1x access control. Use **show dot1x port-control** to display port-based and use **show running-config** to display dot1x port-control-mode port-based single-host.

Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting single-host, only one user can be permitted to use the network still.

Examples

The following example sets the port to participate in authentication and enable port-based authentication:

```
DES-7200(config)# interface g0/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config-if)# dot1x port-control-mode
port-based
DES-7200(config-if)# end
DES-7200#
```

The following example sets 802.1x authentication of single user port:

```
DES-7200(config)# interface g 0/1

DES-7200(config-if)# dot1x port-control auto

DES-7200(config-if)# dot1x port-control-mode

port-based single-host

DES-7200(config-if)# end

DES-7200#
```

Related commands

Command	Description
show dot1x port-control	Show the port control mode.
Show running-config	Show the configuration.

4.5.20 dot1x stationarity enable

In the port-based 802.1X control mode, dynamic users can transit freely among the ports by default. In special cases, if you want to prevent the user from transiting from 802.1X port to other port, you can use the following commands:

dot1x stationarity enable

no dot1x stationarity enable

Parameter description	N/A.
Default configuration	Dynamic users can transit freely among the ports.
Command mode	Global configuration mode.
Usage guidelines	This command must be configured before user authentication. Otherwise, you need re-authenticate all the users.

Examples	The following example prevents the user from transiting from 802.1X port to other port:
	`DES-7200# configure terminal`
	`DES-7200(config)# dot1x stationarity enable`
	`DES-7200(config)# end`
	`DES-7200#`

4.5.21 dot1x redirect url

Use this command to set the redirect url. Before the 802.1x authentication success/failure for the terminal user, if the browser is used to access the network, the switch will redirect the URL accessed by the user to the configured URL, which is began with http://, take http://DES-7200.net/web for example. It is worth mentioning that only http:// is supported and only one redirection address can be configured. The latter url address will cover the former one. Use the **no** form of this command to delete the redirect url address.

dot1x redirect url *[url-string]*

no dot1x redirect url

Parameter description

Parameter	Description
url-string	The URL address.

Default N/A

Command mode Privileged EXEC mode.

Usage guidelines N/A

Examples The following example redirects the network address: DES-7200.net/web:

```
DES-7200# configure terminal
DES-7200(config)# dot1x redirect url
http://DES-7200.net/web
```

Related commands

Command	Description
dot1x redirect for special tcp-destination port	Set the specific destination port and redirect the web request for the destiantion IP.
dot1x redirect time-out	Set the timeout time maintaining the redirect connection.
dot1x redirect num for special source-ip	Set the allowed number of redirect connection of the same source.
show dot1x	Show the dot1x redirection information.

4.5.22 dot1x redirect for special tcp-destination port

Use this command to set the specific destination port and redirect the web request for the destiantion IP. Excepting for the port number 80 and 8080, 16 TCP destination port numbers are supported at most. Use the **no** form of this command to delete the configured redirect port numbers.

[no] dot1x redirect for special tcp-destination port *port num*

Parameter description

Parameter	Description
port-num	TCP destination port number.

Default The default TCP destination port number is 80 and 8080.

Command mode Privileged EXEC mode.

Usage guidelines The valid TCP port number range is 1-65535.

Examples The following example sets the redirect tcp destination port as 8443:

```
DES-7200# configure terminal
DES-7200(config)# dot1x redirect for special
tcp-destination port 8443
```

Related commands

Command	Description
dot1x redirect url	Set the redirect url address.
dot1x redirect time-out	Set the timeout time maintaining the redirect connection.
dot1x redirect num for special source-ip	Set the allowed number of redirect connection of the same source.
show dot1x	Show the dot1x redirection information.

4.5.23 dot1x redirect time-out

Use this command to set the timeout time maintaining the redirect connection. Use the **no** form of this command to restore to the default value.

dot1x redirect time-out port *time-out-interval*

no dot1x redirect time-out port

Parameter description

Parameter	Description
time-out-interval	The timeout time, in seconds. The valid range is 1-10s.

Default	The default value is 3.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A
Examples	The following example set the redirect timeout time as 5s: `DES-7200(config)# dot1x redirect time-out 5`

Related commands

Command	Description
dot1x redirect url	Set the redirect url address.
dot1x redirect for special tcp-destination port	Set the specific destination port and redirect the web request for the destiantion IP.
dot1x redirect num for special source-ip	Set the allowed number of redirect connection of the same source.
show dot1x	Show the dot1x redirection information.

4.5.24 dot1x redirect num for special source-ip

Use this command to set the allowed number of redirect connection of the same source. Use the **no** form of this command to restore to the default value.

dot1x redirect num for special source-ip *num*

no dot1x redirect num for special source-ip

Parameter description

Parameter	Description
num	The redirect connection number. The valid range is 1-10.

Default	1

Command mode	Privileged EXEC mode.
Usage guidelines	N/A
Examples	The following example set the redirect connection number as 3: `DES-7200(config)# dot1x redirect num for special source-ip 3`

Related commands

Command	Description
dot1x redirect url	Set the redirect url address.
dot1x redirect for special tcp-destination port	Set the specific destination port and redirect the web request for the destiantion IP.
dot1x redirect time-out	Set the timeout time maintaining the redirect connection.
show dot1x	Show the dot1x redirection information.

4.6 Show Related Commands

4.6.1 show dot1x

Use this command to display the information about 802.1x setting.

show dot1x

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples

The following example shows the information about 802.1x:

```
DES-7200# show dot1x

802.1X Status:          Enabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       3600 sec
Quiet Timer Period:     10 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
DES-7200#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.

	dot1x timeout tx-period	Set the retransmission period.

4.6.2 show dot1x auth-address-table

Use this command to display 802.1X authentication-allowed address table.

show dot1x auth-address-table[**address** *mac-addr*][**interface** *interface-id*]

Parameter description

Parameter	Description
mac-addr	Physical IP address that can be authenticated
interface	Interface number

Default N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples The following example shows the 802.1x authentication-allowed address table.:

```
DES-7200# show dot1x auth-address-table
interface:g3/1
---------------------------------
mac-addr 00D0.F800.0001
DES-7200#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.

dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

4.6.3 show dot1x auto-req

Use this command to show the configuration information of automatic 802.1x authentication.

show dot1x auto-req

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about automatic 802.1x authentication:
	`DES-7200# show dot1x auto-req`
	`Auto-Req: Disabled`
	`User-Detect : Enabled`
	`Packet-Num : 0`
	`Req-Interval: 30 Seconds`
	`DES-7200#`

	Command	Description
Related commands	**dot1x auth-mode**	Set the 802.1x authentication mode.
	dot1x max-req	Set the maximum number of authentication request retransmissions.
	dot1x port-control auto	Set the port to participate in authentication.
	dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Set the re-authentication attribute.
	dot1x timeout quiet-period	Set the time the device waits before reauthentication.
	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

4.6.4 show dot1x private-supplicant-only

Use this command to show the information about the private supplicant.

show dot1x private-supplicant-only

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.

Usage guidelines	N/A.

Examples	The following example shows the information about the private supplicant:
	`DES-7200# show dot1x private-supplicant-only`
	`private-supplicant-only:: disabled`
	`DES-7200#`

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

4.6.5 show dot1x max-req

Use this command to show the maximum number of authentication request retransmissions to the client.

show dot1x max-req

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the maximum number of authentication request retransmissions:
	`DES-7200# show dot1x max-req`
	`max-req: 2 times`
	`DES-7200#`

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.

	dot1x timeout tx-period	Set the retransmission period.

4.6.6 show dot1x port-control

Use this command to show the ports that participate in authentication.

show dot1x port-control [**interface** *interface*]

Parameter description

Parameter	Description
interface	Specified interface

Default N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples

The following example shows the ports that participate in the authentication:

```
DES-7200# show dot1x port-control
Interface Mode       Dynamic-User Static-User Max-User
Authened  Mab
--------- ---------- ------------ ----------- --------
-------- ---------
Fa0/5     mac-based   0             1           6000
yes
disable
DES-7200#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x	Set the maximum number of the

reauth-max	supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

4.6.7 show dot1x probe-timer

Use this command to show the online probing configurations.

show dot1x probe-timer

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the online probing configuration:
	`DES-7200# show dot1x probe-timer`
	`Hello Interval: 20 Seconds`
	`Hello Alive: 250 Seconds`
	`DES-7200#`

Related	Command	Description

commands	**dot1x auth-mode**	Set the authentication mode.
	dot1x max-req	Set the maximum number of authentication request retransmissions**.**
	dot1x port-control auto	Set the port to participate in authentication.
	dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Set the re-authentication attribute.
	dot1x timeout quiet-period	Set the time the device waits before reauthentication.
	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

4.6.8 show dot1x re-authentication

Use this command to show re-authentication configuration.

show dot1x re-authentication

Parameter description	N/A
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about reauthentication:
	`DES-7200# show dot1x re-authentication`
	`eauth-enabled: disabled`
	`DES-7200#`

Related commands	**Command**	**Description**
	dot1x auth-mode	Set the authentication mode.
	dot1x max-req	Set the maximum number of authentication request retransmissions**.**
	dot1x port-control auto	Set the port to participate in authentication.
	dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Set the re-authentication attribute.
	dot1x timeout quiet-period	Set the time the device waits before reauthentication.
	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

4.6.9 show dot1x reauth-max

Use this command to show the maximum number of re-authentications.

show dot1x reauth-max

Parameter description	N/A.
Default	N/A.

Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about the maximum number of re-authentications:
	`DES-7200# show dot1x reauth-max`
	`reauth-max: 2 times`
	`DES-7200#`

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

4.6.10 show dot1x summary

Use this command to display the 802.1X authentication summary.

show dot1x summary

Parameter description	N/A
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples

The following example shows the summary of 802.1x authentication:

```
DES-7200# show dot1x summary
ID        User         MAC             Interface VLAN
Auth-State
Backend-State Port-Status User-Type Time
--------  ----------  --------------   ---------  ----
--------------  ------------  -----------  ---------
------------------
2           ts-user     0023.aeaa.4286   Fa0/5       1
Authenticated
Idle          Authed      static    0days 0h 8m 8s
DES-7200#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.

dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

4.6.11 show dot1x user id

Use this command to display the information about the 802.1X authentication user.

show dot1x user id <*id*>

Parameter description

Parameter	Description
id	User ID

Default N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples

The following example shows the information about the 802.1x authentication user:

```
DES-7200# show dot1x user id 1
User name: caikov
id: 1
Type: static
Mac address is 0013.2049.8272
Vlan id is 217
Access from port Gi0/13
User ip address is 192.168.217.64
Max user number on this port is 6000
COS on this port is 5
Up-bandwidth is 1024 kbps
Down-bandwidth is 1024 kbps
Authorization vlan is dep7
```

```
Authorization seesion time is 1000000 seconds
Authorization ip address is 192.168.217.64
Start accounting
Permit proxy user
Permit dial user
IP privilige is 2

DES-7200#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

4.6.12 show dot1x timeout

The commands show the information about the 802.1X timeout.

show dot1x timeout quiet-period

show dot1x timeout re-authperiod

show dot1x timeout server-timeout

show dot1x timeout supp-timeout

show dot1x timeout tx-period

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about the time for the device to wait before reauthentication:
	`DES-7200# show dot1x timeout quiet-period`
	`quiet-period: 60 sec`
	DES-7200#

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

5 Port-based Flow Control Configuration Commands

5.1 Configuration Related Commands

5.1.1 protected-ports route-deny

Use this command to configure the L3 routing between the protected ports. Use the **no** form of the command to disable theL3 routing.

protected-ports route-deny

no protected-ports route-deny

Default configuration	Enabled.
Command mode	Global configuration mode.
Usage guidelines	After setting some ports as the protected ports, they can route on L3. Use this command to deny the L3 communication between protected ports. Use **show running-config** to display configuration.
Examples	`DES-7200(config)# protected-ports route-deny`

Related commands

Command	Description
show running-config	Show whether the route-deny between protected ports has been configured.

5.1.2 storm-control

Use this command to enable the storm suppression. Use the **no** form of the command to disable the storm suppression.

storm-control {broadcast | multicast | unicast} [{level *percent* | **pps** *packets*|*rate-bps***}]**

no storm-control {broadcast|multicast|unicast}[{level *percent* | **pps** *packets*|*rate-bps***}]**

Parameter description

Parameter	Description
broadcast	Enable the broadcast storm suppression function.
multicast	Enable the unknown unicast storm suppression function.
unicast	Enable the unknown unicast storm suppression function.
percent	According to the bandwidth percentage to set, for example, 20 means 20%
packets	According to the pps to set, which means packets per second
Rate-bps	rate allowed
64k-2M	In the unit of 64k
2-100M	in the unit of 1M
Above 100M	in the unit of 8M

Default configuration Disabled.

Command mode Interface configuration mode.

Usage guidelines

Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms.

A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

Use **show storm-control** to display configuration.

Examples

The following example enables the multicast storm suppression on GigabitEthernet 1/1 and sets the allowed rate to 4M.

```
DES-7200# configure terminal
DES-7200(config)# interface GigabitEthernet 1/1
DES-7200(config-if)# storm-control multicast 4096
DES-7200(config-if)# end
```

Related commands

Command	Description
show storm-control	Show storm suppression information.

5.1.3 switchport protected

Use this command to configure the interface as protected. Use the **no** form of the command to disable the protected port.

switchport protected

no switchport protected

Default configuration Disabled.

Command mode Interface configuration mode.

Usage guidelines

After these ports are set as the protected ports, they cannot switch on L2 but can route on L3. A protected port can communicate with an unprotected port. Use **show interfaces** to display configuration.

Examples

```
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)# switchport protected
```

Related commands

Command	Description
show interfaces	Show the interface information.

5.1.4 switchport port-security

Use this command to configure port security and the way to deal with violation. Use the **no** form of the command to disable the port security or restore it to the default.

switchport port-security [violation {protect | restrict | shutdown}]

no switchport port-security [violation]

Parameter description

Parameter	Description
port-security	Enable interface security.
violation protect	Discard the packets breaching security.
violation restrict	Discard the packets breaching security and send the Trap message.
violation shutdown	Discard the packets breaching the security, send the Trap message and disable the interface.

Default configuration Disabled.

Command mode Interface configuration mode.

Usage guidelines

With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.

Examples

This example shows how to enable port security on interface gigabitethernet 1/1, and the way to deal with violation is **shutdown**:

```
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security violation shutdown
```

Related commands

Command	Description
show port-security	Show port security settings.

5.1.5 switchport port-security aging

Use this command to set the aging time for all secure addresses on a interface. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface. Use the **no** form of the command to apply the aging time on automatically learned address or to disable the aging.

switchport port-security aging {static | time *time* }

no switchport port-security aging {static | time }

Parameter description

Parameter	Description
static	Apply the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.
time *time*	Specify the aging time for the secure address on this port. Its range is 0-1440 in minutes. If you set it to 0, the aging function is disabled actually.

Default configuration

No secure address is aged.

Command mode

Interface configuration mode.

Usage guidelines

In interface configuration mode, use **no switchport port-security aging time** to disable the aging for security addresses on the port. Use the **no switchport port-security aging static** to apply the aging time to only the dynamically learned security address.

Use **show port-security** to display configuration.

Examples

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# switchport port-security aging time 8
DES-7200(config-if)# switchport port-security aging static
```

Related commands

Command	Description
show port-security	Show port security settings.

5.1.6 switchport port-security binding

Use this command to configure secure address binding manually in the interface configuration mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded. Use the **no** form of the command to remove the binding addresses.

[**no**] **switchport port-security binding** *mac-address* **vlan** *vlan_id ipv4-address* | *ipv6-address*

[**no**] **switchport port-security binding** *ipv4-address* | *ipv6-address*

Parameter description

Parameter	Description
mac-address	Binding source MAC address
vlan_id	Vlan id of the binding source MAC addess
ipv4-address	Binding ipv4 adderess
ipv6-address	Binding ipv6 address

Default configuration N/A

Command mode Interface configuration mode.

Usage guidelines N/A

Examples

1.This example shows how to bind the IP address *192.168.1.100* on the interface *g 0/10:*

```
DES-7200(config)#inter g0/10
DES-7200(config-if)# switchport port-security binding 192.168.1.100
```

2.This example shows how to bind the IP address *192.168.1.100* and MAC address *00d0.f800.5555 w*ith vlan id *1* on the interface *g 0/10*

```
DES-7200(config)#inter g0/10
DES-7200(config-if)# switchport port-security binding 00d0.f800.5555 vlan 1 192.168.1.100
```

Related commands

Command	Description
show port-security	Show port security settings.

switchport port-security	Enable the port-security.
switchport port-security binding interface	Configure the secure address binding in the privileged mode.
Switchport port-security mac-address	Set the static secure address.
switchport port-security aging	Set the aging time for secure address.

5.1.7 switchport port-security binding interface

Use this command to configure secure address binding manually in the privileged mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded. Use the **no** form of the command to remove the binding addresses

[**no**] **switchport port-security binding interface** i*nterface-id mac-address* **vlan** *vlan_id ipv4-address* | *ipv6-address*

[**no**] **switchport port-security binding interface** i*nterface-id ipv4-address* | *ipv6-address*

Parameter description

Parameter	Description
interface-id	Binding interface ID
mac-address	Binding source MAC address
Vlan_id	Vlan ID of the binding source MAC addess
ipv4-address	Binding ipv4 adderess
ipv6-address	Binding ipv6 address

Default configuration N/A

Command mode Privileged mode.

Usage guidelines	N/A

Examples	1.This example shows how to bind the IP address *192.168.1.100* on the interface *g 0/10:*
	`DES-7200(config)# switchport port-security binding interface g 0/10 192.168.1.100`
	2.This example shows how to bind the IP address *192.168.1.100* and MAC address *00d0.f800.5555 w*ith vlan id *1* on the interface *g 0/10*
	`DES-7200(config)# switchport port-security binding interface g 0/10 00d0.f800.5555 vlan 1 192.168.1.100`

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding in the interface configuration mode.
Switchport port-security mac-address	Set the static secure address.
switchport port-security aging	Set the aging time for secure address.

5.1.8 switchport port-security mac-address

Use this command to configure manually the static secure address in the interface configuration mode. Use the **no** form of the command to remove the configuration.

[**no**] **switchport port-security mac-address** *mac-address* [*vlan vlan-id*]

Parameter description

Parameter	Description
mac-address	Static secure MAC address.
vlan-id	Vlan ID of the MAC address. Note: the configuration of vlan-id is only supported on the TRUNK port.

Default configuration N/A.

Command mode Interface configuration mode.

Usage guidelines N/A.

Examples The example below describes how to configure a static secure address 00d0.f800.5555 with VID 2 for interface *g 0/10*:

```
DES-7200(config)#inter g0/10
DES-7200(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding.
switchport port-security mac-address interface	Set the static secure address in the privileged mode.
switchport port-security aging	Set the aging time for the secure address.

5.1.9 switchport port-security mac-address interface

Use this command to configure manually the static secure address in the privileged mode. Use the **no** form of the command to remove the configuration.

[**no**] **switchport port-security interface** i*nterface-id* **mac-address** *mac-address* [*vlan vlan-id*]

Parameter description

Parameter	Description
i*nterface-id*	Interface ID.
mac-address	Static secure address

	vlan-id	Vlan ID of the MAC address. Note: the configuration of vlan-id is only supported on the TRUNK port.

Default configuration N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples The example below describes how to configure a static secure address 00d0.f800.5555 with VID 2 for interface *g 0/10*:

```
DES-7200(config)# switchport port-security interface g0/10 mac-address 00d0.f800.5555 vlan 2
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding.
Switchport port-security mac-address	Set the static secure address in the interface configuration mode.
switchport port-security aging	Set the aging time for the secure address.

5.1.10 switchport port-security sticky mac-address

Use this command to configure manually the Sticky MAC secure address in the interface configuration mode. Use the **no** form of the command to remove the configuration.

[**no**] **switchport port-security mac-address sticky *mac-address*** [*vlan vlan-id*]

Use the command without parameters to enable the Sticky MAC address learning. The **no** form of this command disables the Sticky MAC address learning.

[no] switchport port-security mac-address sticky

Parameter description

Parameter	Description
mac-address	Static secure address.
vlan-id	Vlan ID of the MAC address. Note: the configuration of vlan-id is only supported on the TRUNK port.

Default configuration

The Sticky MAC address learning is disabled by default.

Command mode

Interface configuration mode.

Usage guidelines

N/A.

Examples

The example below describes how to configure a static secure address 00d0.f800.5555 with VID 2 for the trunk port *g 0/10*:

```
DES-7200(config)#inter g0/10
DES-7200(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2
```

The example below describes how to enable the Sticky MAC address learning on the interface *g0/10*:

```
DES-7200(config)#inter g0/10
DES-7200(config-if)# switchport port-security sticky mac-address
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding.
switchport port-security mac-address interface	Set the static secure address in the privileged mode.

switchport port-security mac-address	Set the static secure address in the interface configuration mode.
switchport port-security aging	Set the aging time for the secure address.

5.1.11 switchport port-security maximum

Use this command to set the maximum number of the port secure address.. Use the **no** form of the command to restore it to the default setting.

switchport port-security maximum *value*

[**no**] **switchport port-security maximum**

Parameter description

Parameter	Description
value	Maximum number of the secure address, in the range of 1 to 128.

Default configuration 128

Command mode Interface configuration mode.

Usage guidelines The number of the secure address contains the sum of static secure address and dynamically learnt secure address, 128 by default. If the number of the secure address you set is less than current number, it will prompt this setting fails.

Examples The example below describes how to set the maximum number of the secure address as 2 for interface *g 0/10*

```
DES-7200(config)#inter g0/10
DES-7200(config-if)# switchport port-security maximum 2
```

Related commands

Command	Description
show port-security	Show port security settings.

switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding.
Switchport port-security mac-address	Set the static secure address in the interface configuration mode.
switchport port-security aging	Set the aging time for the port secure address.

5.1.12 nac-author-user maximum

Use this command to set the limited number of port IP address. Use the **no** form of the command to disable the port IP address number limit.

nac-author-user maximum *value*

[**no**] **nac-author-user maximum**

Parameter description

Parameter	Description
value	The limited IP address number in the range of 1 to 1024.

Default configuration Disabled.

Command mode Interface configuration mode.

Usage guidelines If the limited number of the IP address you set is less than bound number, it will prompt this setting fails.

Examples The example below describes how to set the limited number of the port IP address as 100

```
DES-7200(config)#inter f 0/1
DES-7200(config-if)#nac-author-user maximum 100
```

Related commands	Command	Description
	show nac-author-user	Show the limited and bound number of IP address on the port.

5.2 Showing Related Commands

5.2.1 show nac-author-user

Use this command to show the limited and bound number of IP address on the port.

show nac-auth-user

Parameter description	Parameter	Description
	-	-

Default configuration All information is shown by default.

Command mode Privileged mode.

Usage guidelines N/A

Examples

```
DES-7200#show nac-author-user
```

Related commands	Command	Description
	nac-auth-user maximum *value*	Set the limited number of port IP address.

5.2.2 show port-security

Use this command to show port security settings.

show port-security [address] [interface *interface-id***] [all]**

Parameter description

Parameter	Description
address	Show all the secure addresses or the secure address on the specified interface.
Interface *interface-id*	Show the port security configuration of the specified interface.
all	Show the port security configuration of all interfaces.

Command mode

Privileged mode.

Usage guidelines

This command shows all the port security configurations, secure addresses and the way to deal with violation if no parameter is configured .

Examples

```
DES-7200# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security Action
-------- -------------- ----------- -----------
Gi1/1 128 1 Restrict
Gi1/2 128 0 Restrict
Gi1/3 8 1 Protect
```

Related commands

Command	Description
switchport port-security	Enable port security and configure the way to deal with violation.
switchport port-security aging	Specify the aging time fpr the secure address on the interface.
switchport port-security mac-address	Configure the secure address table.

5.2.3 show storm-control

Use this command to show storm suppression information.

show storm-control [*interface-id*]

Parameter description

Parameter	Description
interface-id	Interface on which the storm suppression is enabled

Default configuration	All information is displayed.

Command mode	Privileged mode.

Examples

```
DES-7200# show storm-control gigabitethernet 1/1
Interface Broadcast Control Multicast Control Unicast
Control
---------- -------------- ----------------
--------------
Gi1/1 Disabled Disabled Disabled
```

Related commands

Command	Description
storm-control	Enable storm suppression.

6 URPF Configuration Commands

6.1 Configuration Related Commands

6.1.1 ip verify unicast source reachable-via(Global configuration mode)

Use this command to enable the URPF feature in the global configuration mode. Use the **no** form of this command to disable the URPF feature or remove the URPF optional items.

ip verify unicast source reachable-via rx

no ip verify unicast

	Parameter	**Description**
Parameter description	**rx**	URPF check in the strict mode. In the strict mode, the egress port for the forwarding entry in the forwarding list found through the source address for the IP packet shall be matched with the ingress port.

Default Settings	Disabled
Command mode	Global configuration mode.
Usage guidelines	To determine whether the route for the source address is in the forwarding list or not and the packet validity, enable the URPF feature to check the source address for the received IP packets. If no forwarding entry is matched, the packets are illegal.

Enabling URPF feature in the global configuration mode enables URPF check for the received packets on all interfaces.

Caution

1. For DES-7200 series, the global URPF configuration is valid after the MPLS service card has been inserted. After enabling the URPF feature, the URPF check will be enabled for the IPv4 packets.
2. In the global configuration mode, the URPF feature can only be enabled in the strict mode. Howerver, the user can match the equivalent route in the loose mode.
3. In the global configuration mode, the URPF feature does not support the URPF check using the default route.
4. URPF feature cannot be configured in the global configuration mode and in the interface configuration mode at the same time.
5. It is worth mentioning that for DES-7200 series, it is not recommended to configure the URPF in the global configuration mode for the user network directly-connected. If DES-7200 series fails to learn the ARP entries of the directly-connected users before forwarding the packets, the URPF check fails and the datagrams are dropped.

Examples

The following example shows how to enable the URPF feature globally:

```
DES-7200(config)# ip verify unicast source reachable-via rx
```

Related commands

Command	Description
show ip urpf	Show the URPF information.

Platform description

This command is supported on the DES-7200 series MPLS line card only.

6.1.2 ip verify unicast source reachable-via(Interface configuration mode)

Use this command to enable the URPF feature in the interface configuration mode. Use the **no** form of this command to disable the URPF feature or remove the URPF optional items.

ip verify unicast source reachable-via {**rx** | **any**} [**allow-default** | *acl_name*]

no ip verify unicast

Parameter description

Parameter	Description
rx	URPF check in the strict mode. In the strict mode, the egress port for the forwarding entry in the forwarding list found through the source address for the IP packet shall be matched with the ingress port.
any	URPF check in the loose mode. In the loose mode, the forwarding entry for the source address for the IP packet can be found in the forwarding list.
allow-default	(Optional) Allow to use the default route to check URPF.
acl_name	(Optional) Set the ACL number: 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)

Default Settings Disabled

Command mode Interface configuration mode.

Usage guidelines

To determine whether the route for the source address is in the forwarding list or not and the packet validity, enable the URPF feature to check the source address for the received IP packets. If no forwarding entry is matched, the packets are illegal.

Enabling URPF feature in the interface configuration mode enables URPF check for the received packets on the interface.

By default, the default route is not used for URPF check. Use the keyword allow-default to enable the URPF check.

By default, the packets failed to pass the URPF check are dropped. With ACL(acl-name) configured, the ACL matching continues when the routing fails. The packets will be dropped if the ACL is inexistent or the deny ACE is matched; otherwise, if the permit ACE is matched, the packets will be forwarded.

↙ Caution

1. With this command configured, for the switch product(DES-7200 series), the URPF check is enabled for the IPv4/IPv6 packets; while for the routers, the URPF check is enabled for the IPv4 packets.

2. For the switch product, the URPF feature is supported only on the B-category linecard-related Routed Port and L3 AP on the DES-7200 series. The restrictions of the URPF feature are as follows:

Not support the ACL association;

Not support to use the IPv6 route with prefix in 65~127 bits for the URPF check;

After enabling the URPF feature, the range of packets received on the interface will be expanded, that is, the URPF feature is enabled for all packets received on the physical ports.

After enabling the URPF feature, it halves the route forwarding capacity.

After enabling the URPF feature in the strict mode, the user can match the equivalent route when URPF check is enabled for the packets received on the interface.

For the DES-7200 series with MPLS service card inserted, the URPF feature cannot be configured on the interface.

3. URPF feature cannot be configured in the global configuration mode and in the interface configuration

	mode at the same time.

Examples	The following example shows how to check the URPF feature of the received packets in the strict mode on the interface GigabitEthernet 0/21
	`DES-7200(config)# interface gigabitEthernet0/21`
	`DES-7200(config-if)# ip verify unicast source reachable-via rx`

Related commands

Command	Description
show ip urpf	Show the URPF information.

Platform description	DES-7200 series class-B line cards.

6.1.3 ip verify urpf drop-rate compute interval

Use this command to set the URPF drop-rate compute interval. Use the **no** form of this command to restore it to the default value.

ip verify urpf drop-rate compute interval *seconds*

no ip verify urpf drop-rate compute interval

Parameter description

Parameter	Description
seconds	Set the URPF drop-rate compute interval, in seconds. The valid range is 30-300.

Default Settings	30s
Command mode	Global configuration mode.
Usage guidelines	N/A
Examples	The following example shows how to set the URPF drop-rate compute interval as 1 minute:

```
DES-7200(config)# ip verify urpf drop-rate compute
interval 60
```

Related commands

Command	Description
ip verify urpf drop-rate notify	Set the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Set the URPF drop-rate warning interval.
ip verify urpf notification threshold	Set the URPF drop-rate threshold.

6.1.4 ip verify urpf drop-rate notify

Use this command to enable the URPF drop-rate information monitoring. Use the **no** form of this command to disable this function.

ip verify urpf drop-rate notify

no ip verify urpf drop-rate notify

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Interface configuration mode.

Usage guidelines

This command is used to enable the URPF drop-rate information monitoring, notifying the user of the URPF packet drop information by means of Syslog or Trap for the convenience of the user network monitoring.

Examples

The following example shows how to enable the URPF drop-rate information monitoring on the interface GigabitEthernet 0/21:

```
DES-7200(config)# interface gigabitEthernet0/21
DES-7200(config-if)# ip verify urpf drop-rate notify
```

	Command	Description
Related commands	**ip verify urpf drop-rate compute interval**	Set the URPF drop-rate compute interval.
	ip verify urpf drop-rate notify hold-down	Set the URPF drop-rate warning interval.
	ip verify urpf notification threshold	Set the URPF drop-rate threshold.

6.1.5 ip verify urpf drop-rate notify hold-down

Use this command to set the URPF drop-rate warning interval. Use the **no** form of this command to restore it to the default value.

ip verify urpf drop-rate notify hold-down *seconds*

no ip verify urpf drop-rate notify hold-down

	Parameter	Description
Parameter description	*seconds*	Set the URPF drop-rate warning interval, in seconds. The valid range is 30-300.

Default Settings	300s
Command mode	Global configuration mode.
Usage guidelines	N/A
Examples	The following example shows how to set the URPF drop-rate warning interval as 1 minute: `DES-7200(config)# ip verify urpf drop-rate notify hold-down 60`

	Command	Description
Related commands	**ip verify urpf drop-rate compute interval**	Set the URPF drop-rate compute interval.
	ip verify urpf drop-rate notify	Set the URPF drop-rate information monitoring.
	ip verify urpf notification threshold	Set the URPF drop-rate threshold.

6.1.6 ip verify urpf notification threshold

Use this command to set the URPF drop-rate threshold. Use the **no** form of this command to restore it to the default value.

ip verify urpf notification threshold *rate-value*

no ip verify urpf notification threshold

	Parameter	Description
Parameter description	rate-value	Set the URPF drop-rate threshold, in pps(packets per second). The valid range is 0-4294967295.

Default Settings	1000pps
Command mode	Interface configuration mode.
Usage guidelines	The threshold 0 indicates that once monitoring the dropped packet due to the URPF check, the notification is sending. The user can adjust the drop-rate threshold value according to the actual network application.
Examples	The following example shows how to set the URPF drop-rate threshold 10pps on the interface GigabitEthernet 0/21:

```
DES-7200(config)# interface gigabitEthernet0/21
DES-7200(config-if)# ip verify urpf drop-rate notify
DES-7200(config-if)# ip verify urpf notification
threshold 10
```

Related commands

Command	Description
ip verify urpf drop-rate compute interval	Set the URPF drop-rate compute interval.
ip verify urpf drop-rate notify	Set the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Set the URPF drop-rate warning interval.

6.1.7 snmp-server enable traps

Use this command to enable the URPF Trap notification if the URPF drop-rate exceeds the threshold value. Use the **no** form of this command to disable this function.

snmp-server enable traps [urpf]

no snmp-server enable traps [urpf]

Parameter description

Parameter	Description
urpf	Enable the URPF Trap notification.

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

By default, when the URPF drop-rate exceeds the threshold value, it auto-notifies the user by means of Syslog. However, after configuring this command, the URPF Trap notification is enabled.

Examples

```
DES-7200(config)# snmp-server enable traps urpf
```

Related commands	Command	Description
	snmp-server host	Specify the SNMP host.
	ip verify urpf drop-rate compute interval	Set the URPF drop-rate compute interval.
	ip verify urpf drop-rate notify	Set the URPF drop-rate information monitoring.
	ip verify urpf drop-rate notify hold-down	Set the URPF drop-rate warning interval.
	ip verify urpf notification threshold	Set the URPF drop-rate threshold.

6.1.8 snmp-server host traps

Use this command to specify the SNMP host(NMS) to receive the URPF Trap message in the global configuration mode. Use the **no** form of this command to remove the specofied SNMP host.

snmp-server host {*host-addr*| **ipv6** *ipv6-addr*} **traps** *community-string* [**urpf**]

no snmp-server host {*host-addr*| **ipv6** *ipv6-addr*} **traps** *community-string*

Parameter description	Parameter	Description
	host-addr	Set the SNMP host address.
	ipv6-addr	Set the SNMP IPv6 address.
	community-string	Set the community string or username(Version3)
	urpf	URPF Trap.

Default Settings	By default, no SNMP host is specified. If the trap type is not specified, all trap types are included.
Command mode	Global configuration mode.

Usage guidelines	Use this command and the **snmp-server enable traps** command to send the URPF Trap messages to the specified NMS.
Examples	The following example shows how to specify the SNMP host 192.168.12.219 to send the URPF Trap message: `DES-7200(config)# snmp-server host 192.168.12.219 public urpf`

Related commands

Command	Description
snmp-server enable traps	Enable to send the Trap message.
ip verify urpf drop-rate compute interval	Set the URPF drop-rate compute interval.
ip verify urpf drop-rate notify	Set the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Set the URPF drop-rate warning interval.
ip verify urpf notification threshold	Set the URPF drop-rate threshold.

6.2 Showing Related Commands

6.2.1 show ip urpf

Use this command to show the URPF configuration and the statistical information.

show ip urpf [**interface** *interface-name*]

Parameter description

Parameter	Description
interface *interface-name*	Show the configurations and the statistical information on the specified interface.

Default Settings	N/A

Command mode	Privileged EXEC mode.
Usage guidelines	Without an interface specified, the global configurations and the statistical information or those of all interfaces are shown.
Examples	DES-7200# **show ip urpf interface** *gigabitEthernet0/21* IP verify source reachable-via RX IP verify URPF drop-rate notify disabled IP verify URPF notification threshold is 1000pps Number of drop packets in this interface is 124 Number of drop-rate notification counts in this interface is 0

Related commands

Command	Description
ip verify unicast source reachable-via	Enable the URPF features.
ip verify urpf drop-rate compute interval	Set the URPF drop-rate compute interval.
ip verify urpf drop-rate notify hold-down	Set the URPF drop-rate warning interval.
ip verify urpf notification threshold	Set the URPF drop-rate threshold.
clear ip urpf	Clear the URPF statistical information.

6.3 Clearing Related Commands

6.3.1 clear ip urpf

Use this command to clear the URPF statistical information on the number of dropped packets.

clear ip urpf [**interface** *interface-name*]

Parameter description

Parameter	Description
interface *interface-name*	Show the statistical information on the specified interface.

Default Settings

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

Without an interface specified, the statistical information of all interfaces are cleared.

Examples

```
DES-7200# show ip urpf interface gigabitEthernet0/21
IP verify source reachable-via RX
IP verify URPF drop-rate notify disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface
is 0
```

Related commands

Command	Description
showip urpf	Show the URPF configurations and statistical information.

7 CPU Protection Configuration Commands

7.1 Related Configuration Commands

7.1.1 cpu-protect type packet-type pps pps_value

Use this command to set the bandwidth for the CPU port to receive the specified type of packets.

cpu-protect type { **arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **ttl1** | **unknown-ipmc** | **dvmrp|…** } **pps** *pps_value*

Parameter description

Parameter	Description
pps_value	Packets per second.

Default

The default bandwidth that the CPU uses to receive various types of packets is 1000 pps.

Command mode

Global configuration mode.

Examples

The following example sets the bandwidth for the CPU to receive BPDU packets as 100pps:

```
DES-7200(config)# cpu-pr type bpdu pps 100
Set packet type bpdu pps 100.
```

Related commands

Command	Description
cpu-protect type packet-type pri *pri_num*	Set the priority for the packets the CPU port receives.

7.1.2 cpu-protect type packet-type pri *pri_num*

Use this command to set the priority for the specified type of packets the CPU port receives.

cpu-protect type { **arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **ttl1** | **unknown-ipmc** | **dvmrp|…** } **pri** *pri_num*

Parameter description

Parameter	Description
pri_num	Packet priority in the range 0 to 7

Default The default is 0 for various types of packets.

Command mode Global configuration mode.

Examples The following example sets the priority of the BPDU packets as 7:

```
DES-7200(config)# cpu-protect type bpdu pri 7
Set packet type bpdu pri 7.
```

Related commands

Command	Description
cpu-protect type packet-type pps *pps_value*	Set the bandwidth for the CPU to receive the specified type of packets.

7.2 Showing Related Commands

7.2.1 show cpu-protect mboard

Use this command to show the statistics of various packets of CPU protection on the management board.

show cpu-protect mboard

Command mode Privileged EXEC mode.

Usage guidelines This command shows the statistics of the packets received by CPU on the management board.

Examples

The following example shows the statistics of the CPU protection

```
DES-7200# show cpu-protect mboard
 Type            Pps      Total    Drop
 ------------    -------- ------- ---------
 arp             500       19       0
 bpdu            200       24       0
 dhcp            0         0        0
 gvrp            0         0        0
 ipv6-mc         0         0        0
 dvmrp           0         0        0
 igmp            0         0        0
 ospf            0         0        0
 pim             0         0        0
 rip             0         0        0
 vrrp            0         0        0
 unknown-ipmc    0         0        0
 ttl1            0         0        0
...
```

Related commands

Command	Description
show cpu-protect slot *slot-num*	Show the statistics of the CPU protection on the specified line card.

7.2.2 show cpu-protect slot

Use this command to show the CPP statistics on the specified line card.

show cpu-protect slot *slot_num*

Parameter description

Parameter	Description
slot_num	1-16.

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the CPP statistics on the specified line card.

Examples

The following example shows the CPU protection information on the line card in slot 2.

```
DES-7200(config)# show cpu-protect slot 2
 Type          Pps      Total    Drop
```

```
-----------  --------- --------- ---------
arp          200       200       15
bpdu         200       8         0
dhcp         200       0         0
gvrp         200       0         0
ipv6-mc      200       0         0
dvmrp        200       0         0
igmp         200       0         0
ospf         200       0         0
pim          200       0         0
rip          200       0         0
vrrp         200       0         0
unknown-ipmc 200       0         0
ttl1         20        3         0
```

Related commands

Command	Description
show cpu-protect mboard	Show the CPU protect information on the management board.

7.2.3 show cpu-protect type

Use this command to show the statistics of the specified type of packets:

show cpu-protect type { **arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **ttl1** | **unknown-ipmc** | **dvmrp|…** } *dvmrp*

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the statistics of the specified type of packets:

Examples

The following example shows the statistics of the BPDU packets by using the **show cpu-protect type bpdu** command:

```
DES-7200(config)# show cpu-protect type arp
 Slot        Type        Pps       Total     Drop
 ---------   ---------- --------- --------- ---------
 MainBoard   bpdu         100       30        0
 Slot-2      bpdu         100       30        0
```

Related commands

Command	Description
show cpu-protect	Show the statistics of the packets of a specified type of CPU protection.

	type *packet-type*	

Caution	The "…" symbol in the CPP configuration commands means the unlisted CPP types.

8 DoS Protection Configuration Commands

8.1 Configuration Related Commands

8.1.1 ip deny invalid-l4port

Use this command to enable the anti-attack of the self-consumption. Use the **no** form of this command to disable this function.

ip deny invalid-l4port

no ip deny invalid-l4port

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

N/A.

Examples

The following example shows how to enable the anti-attack of the self-consumption:

```
DES-7200(config)# ip deny invalid-l4port
```

The following example shows how to disable the anti-attack of the self-consumption:

```
DES-7200(config)# no ip deny invalid-l4port
```

Related

Command	Description

	show ip deny invalid-l4port	Show the state of anti-attack of the self-consumption.

8.1.2 ip deny invalid-tcp

Use this command to enable the anti-attack of the invalid TCP packets. Use the **no** form of this command to disable this function.

ip deny invalid-tcp

no ip deny invalid-tcp

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

N/A.

Examples

The following example shows how to enable the anti-attack of the invalid TCP packets:

```
DES-7200(config)# ip deny invalid-tcp
```

The following example shows how to disable the anti-attack of the invalid TCP packets:

```
DES-7200(config)# no ip deny invalid-tcp
```

Related commands

Command	Description
show ip deny invalid-tcp	Show the state of anti-attack of the invalid TCP packets.

8.1.3 ip deny land

Use this command to enable the anti-land-attack. Use the **no** form of this command to disable this function.

ip deny land

no ip deny land

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

N/A.

Examples

The following example shows how to enable the anti-land-attack:

```
DES-7200(config)# ip deny land
```

The following example shows how to disable the anti-land-attack:

```
DES-7200(config)# no ip deny land
```

Related commands

Command	Description
show ip deny land	Show the anti-land-attack state.

8.1.4 ip deny spoofing-source

Use this command to enable the ingress filtering to defend against DoS attack. Use the **no** form of this command to disable this function.

ip deny spoofing-source

no ip deny spoofing-source

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Interface configuration mode.

Usage guidelines	This command takes effect on only the layer 3 interfaces with network addresses configured.

Examples

The following example shows how to enable the ingress filtering on the SVI port:

```
DES-7200(config)# int vlan 1
DES-7200(config-if-vlan)# ip deny spoofing-source
```

The following example shows how to disable the ingress filtering on the SVI port:

```
DES-7200(config)# int vlan 1
DES-7200(config-if-vlan)# no ip deny spoofing-source
```

The following example shows how to enable the ingress filtering on the routed port Fa 0/5:

```
DES-7200(config)# int Fa 0/5
DES-7200(config-if-FastEthernet)# ip deny spoofing-source
```

The following example shows how to disable the ingress filtering on the routed port Fa 0/5:

```
DES-7200(config)# int fa 0/5
DES-7200(config-if- FastEthernet)# no ip deny spoofing-source
```

Related commands

Command	Description
-	-

8.2 Showing Related Commands

8.2.1 show ip deny invalid-l4port

Use this command to show the state of the anti-consumption-attack.

show ip deny invalid-l4port

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	DES-7200# **show ip deny invalid-l4port** DoS Protection Mode State ------------------------------ ----- protect against invalid l4port attack Off

8.2.2 show ip deny invalid-tcp

Use this command to show the state of the anti-attack of the invalid TCP packets.

show ip deny invalid-tcp

Parameter description	**Parameter** / **Description** - / -
Default Settings	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A
Examples	DES-7200# **show ip deny invalid-tcp** DoS Protection Mode State ------------------------------------ ----- protect against invalid tcp attack On
Related commands	**Command** / **Description** (**no**) **ip deny invalid-tcp** / Enable/Disable the anti-attack of the invalid TCP packets.

8.2.3 show ip deny land

Use this command to show the anti-land-attack state.

show ip deny land

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

```
DES-7200# show ip deny land
DoS Protection Mode             State
------------------------------      -----
protect against land attack      On
```

Related commands

Command	Description
(**no**) **ip deny land**	Enable/Disable the anti-land-attack function.

9 DHCP Snooping Configuration Commands

9.1 DHCP Snooping Global Commands

9.1.1 ip dhcp snooping

Use this command to enable the DHCP snooping function globally. The **no** form of this command will disable the DHCP snooping function globally.

[**no**] **ip dhcp snooping**

Parameter description	N/A.
Default	Disabled
Command mode	Global configuration mode
Usage guidelines	Enable the DHCP snooping function on the switch. You can use the **show ip dhcp snooping** command to view whether the DHCP snooping function is enabled. Note that DHCP Snooping cannot coexist with private VLAN.

Examples	The following is an example of enabling the DHCP snooping function.
	`DES-7200# configure terminal`
	`DES-7200(config)# ip dhcp snooping`
	`DES-7200(config)# end`
	`DES-7200# show ip dhcp snooping`
	`Switch DHCP snooping status: ENABLE`
	`DHCP snooping Verification of hwaddr field status: DISABLE`
	`DHCP snooping database write-delay time: 0 seconds`

```
DHCP snooping option 82 status: ENABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface         Trusted         Rate limit (pps)
-----------------------  -------    --------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of DHCP snooping.
ip dhcp snooping vlan	Configure DHCP snooping enabled VLAN.

9.1.2 ip dhcp snooping vlan

Use this command to enable DHCP snooping for the specific VLAN. The **no** form of this command will disable the DHCP snooping function for the corresponding VLAN.

[**no**] **ip dhcp snooping vlan** {*vlan-rng* **|** {*vlan-min* [*vlan-max*]}}

Parameter description

Parameter	Description
vlan-rng	VLAN range of effective DHCP snooping.
vlan-min	Minimum VLAN of effective DHCP snooping.
vlan-max	Maximum VLAN of effective DHCP snooping.

Default

By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

Command mode

Global configuration mode.

Usage guidelines

Use this command to configure effective DHCP snooping VLAN by character string.

Examples

The following example enables the DHCP snooping function in VLAN1000.

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping vlan 1000
```

```
DES-7200(config)# end
```

Related commands

Command	Description
ip dhcp snooping	Global switch of DHCP snooping.

9.1.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP snooping bootp bind function. The **no** form of this command will disable the function.

[**no**] **ip dhcp snooping bootp-bind**

Parameter description N/A.

Default Disabled

Command mode Global configuration mode.

Usage guidelines By default, the DHCP Snooping only forwards Bootp packets. With this function enabled, it can snoop Bootp packets. After the Boop client requests an address successfully, the DHCP Snooping adds the Bootp user to the static binding database.

Examples The following example enables the DHCP snooping bootp bind function.

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping bootp-bind
DES-7200(config)# end
DES-7200# show ip dhcp snooping
Switch DHCP snooping status : ENABLE
Verification of hwaddr field status : DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface            Trusted       Rate limit (pps)
-----------------------  -------    ------------
```

Related

Command	Description

show ip dhcp snooping	Show the configuration of the DHCP snooping.

9.1.4 ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message. The **no** form of this command disables this function.

[**no**] **ip dhcp snooping verify mac-address**

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Use this command to enable checking the validity of the source MAC address of the DHCP request message. Once the function is enabled, the system will discard the DHCP request message that fails to pass the source MAC address check.

Examples	The following is an example of enabling the check of the source MAC address of the DHCP request message.
	`DES-7200# configure terminal`
	`DES-7200(config)# ip dhcp snooping verify mac-address`
	`DES-7200(config)# end`
	`DES-7200# show ip dhcp snooping`
	`Switch DHCP snooping status: ENABLE`
	`Verification of hwaddr field status: ENABLE`
	`DHCP snooping database write-delay time: 0 seconds`
	`DHCP snooping option 82 status: ENABLE`
	`DHCP Snooping Support Bootp bind status: ENABLE`
	`Interface Trusted Rate limit (pps)`
	`----------  -------  ----------`

Related	Command	Description

	show ip dhcp snooping	View the configuration information of the DHCP snooping.

9.1.5 ip dhcp snooping information option

Use this command to add option82 to the DHCP request message. The **no** form of this command disables this function.

[no] ip dhcp snooping information option [standard-format]

Parameter description

Parameter	Description
standard-format	The option82 uses the standard format.

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

This command adds option82 to the DHCP request message based on which the DHCP server assigns IP address.

Examples

Add option82 to the DHCP request message:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping information option
DES-7200(config)# end
DES-7200# show ip dhcp snooping
Switch DHCP snooping  status                 :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time       :   0
DHCP snooping option 82 status               :   DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface             Trusted      Rate limit (pps)
----------------------- -------      ----------------
```

Related commands

Command	Function

	show ip dhcp snooping	Show the configuration of the DHCP Snooping.

9.1.6 ip dhcp snooping information option format remote-id

Use this command to set the option82's sub-option remote-id as the customized character string. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping information option format remote-id [string** *ascii-string* **| hostname]**

Parameter description

Parameter	Description
string	The content of the option82's remote-id extension format is customized character string.
hostname	The content of the option82's remote-id extension format hostname.

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

This command sets the remote-id in the option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the option82 information.

Examples

The following is an example of adding the option82 into the DHCP request packets with the content of remote-id being hostname:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping information option format remote-id hostname
```

Related commands

Command	Description
-	-

9.1.7 ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP snooping binding database into the flash periodically. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping database write-delay** *time*

Parameter description

Parameter	Description
time	The interval at which the system writes the dynamic user information of the DHCP snooping database into the flash.

Default Disabled

Command mode Global configuration mode.

Usage guidelines This function can avoid loss of user information after restart. In that case, users need to obtain IP addresses again for normal communication.

Examples

The following is an example of setting interval at which the switch writes the user information into the flash as 3600s:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping database write-delay
3600
DES-7200(config)# end
DES-7200# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: ENABLE
DHCP snooping database write-delay time: 3600
DHCP snooping option 82 status: DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface         Trusted          Rate limit (pps)
-----------------------  -------     ---------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

9.1.8 ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

ip dhcp snooping database write-to-flash

Parameter description	N/A.
Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

Examples	The following is an example of writing the dynamic user information of the DHCP binding database into flash.
	`DES-7200# configure terminal`
	`DES-7200(config)# ip dhcp snooping database write-to-flash`
	`DES-7200(config)# end`
	`DES-7200#`

Related commands	N/A.

9.2 DHCP snooping Interface Mode Commands

9.2.1 ip dhcp snooping suppression

Use this command to set the port to be the suppression status. The no form of this command will set the port to be no suppression status.

[**no**] **ip dhcp snooping trust**

Parameter description	N/A.

Default	Disabled
Command mode	Interface configuration mode.
Usage guidelines	This command can deny all DHCP request messages under the port, that is, all the users under the port are prohibited to request addresses through DHCP.

Examples	The following is an example of setting **fastethernet** 0/2 to be suppression status:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface fastEthernet 0/2`
	`DES-7200(config-if)# ip dhcp snooping suppression`
	`DES-7200(config-if)# end`

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

9.2.2 ip dhcp snooping trust

Use this command to set the ports of the switch as trusted ports. The no form of this command sets the ports as untrust ports.

[**no**] **ip dhcp snooping trust**

Parameter description	N/A.
Default	All ports are untrust ports.
Command mode	Interface configuration mode.
Usage guidelines	Use this command to set the port as trust port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrust port will be discarded.

Examples

The following is an example of setting **fastEthernet** *0/1* as a trust port:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip dhcp snooping trust
DES-7200(config-if)# end
DES-7200# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP Snooping Support Bootp bind status:ENABLE
Interface          Trusted           Rate limit (pps)
-----------------  -------          ----------------
FastEthernet0/1        yes                unlimited
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

9.2.3 ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan

Use this command to enable the option82's sub-option circuit and change the VLAN in the circuit-id into the specified VLAN. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*

Parameter description

Parameter	Description
vlan	The specified vlan to change.

Default Disabled

Command mode Interface configuration mode.

Usage guidelines

With this command configured, the option82 is added to the DHCP request packets, the circuit-id in the option82 information is the specified VLAN and the DHCP server will assign the addresses according to the option82 information.

Examples

The following is an example of adding the option82 to the DHCP request packets and changing the VLAN4094 in the option82's sub-option circuit-id to VLAN93:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip dhcp snooping vlan 4094
information option change-vlan-to vlan 4093
DES-7200(config-if)# end
```

Related commands

Command	Description
-	-

Platform description

This command is supported on all switches.

9.2.4 ip dhcp snooping vlan *vlan-id* information option format-type circuit-id string

Use this command to configure the option82's sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*

Parameter description

Parameter	Description
vlan-id	The VLAN where the DHCP request packets are.
ascii-string	The user-defined content to fill to the Circuit ID.

Default

Disabled

Command mode

Interface configuration mode.

Usage guidelines	This command is used to add the option82 to the DHCP request packets. The content of the sub-option circuit-id is customized, and the DHCP server will assign the addresses according the option82 information.

Examples

The following is an example of adding the option82 to the DHCP request packets with the content of the sub-option circuit-id being *port-name*:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip dhcp snooping vlan 4094 information option format-type circuit-id string port-name
DES-7200(config-if)# end
```

Related commands

Command	Description
-	-

Platform description

This command is supported on all switches.

9.2.5 ip dhcp snooping limit rate

Use this command to set rate limit of receiving DHCP packets on the interface. The **no** form of this command removes the setting.

[**no**] **ip dhcp snooping limit rate** *rate-value*

Parameter description

Parameter	Description
rate-value	Rate of receiving DHCP packets (pps).

Default

No rate limit.

Command mode

Interface configuration mode.

Usage guidelines	This function takes effect for all the interfaces of the VLAN controlled by the DHCP Snooping, including trust interface. For some CPP-enabled products, CPP will restrict the rate of DHCP packets by hardware. CCP-based rate limit takes precedence over DHCP Snooping-based rate limit. For CPP, please refer to specific chapters. You can view the rate limit setting on the corresponding interface by **show ip dhcp snooping** command. Note that DES-7200 does not support rate limit of DHCP packets on an interface.

Examples

The following example sets rate limit of port 1 as 100:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip dhcp snooping limit rate 100
DES-7200(config-if)# end
DES-7200# show ip dhcp snooping
Switch DHCP snooping  status: ENABLE
DHCP snooping  Verification of hwaddr field status:
DISABLE
DHCP snooping database write-delay time:0 seconds
DHCP snooping option 82 status:ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface               Trusted      Rate limit (pps)
----------------------  -------      ----------------
GigabitEthernet 0/1        NO             100
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

Platform description	This command is supported on all switches.

9.3 Showing Related Commands

9.3.1 show ip dhcp snooping

Use this command to view the setting of the DHCP snooping.

show ip dhcp snooping

Parameter description N/A.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples

Show the information of DHCP Snooping.

```
DES-7200# show ip dhcp snooping
Switch DHCP snooping status : ENABLE
Verification of hwaddr field status : DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                Trusted    Rate limit (pps)
-----------------------  -------    ------------
```

Related commands

Command	Description
ip dhcp snooping	Enable the DHCP snooping globally.
ip dhcp snooping verify mac-address	Enable the check of source MAC address of DHCP Snooping packets.
ip dhcp snooping write-delay	Set the interval of writing user information to FLASH periodically.
ip dhcp snooping information option	Add option82 to the DHCP request message.
ip dhcp snoooping bootp-bind	Enable the DHCP snooping bootp bind function.
ip dhcp snooping trust	Set the port as a trust port.

9.3.2 show ip dhcp snooping binding

Use this command to view the information of the DHCP snooping binding database.

show ip dhcp snooping binding

Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples	Show the information of the DHCP Snooping binding database.
	`DES-7200# show ip dhcp snooping binding`
	`Total number of bindings: 1`
	`MacAddress IpAddress Lease Type VLAN Interface`
	`00d0.f801.0101 192.168.1.1 - static 1 fastethernet 0/1`

Related commands

Command	Description
ip dhcp snooping binding	Add the static user information to the DHCP Snooping database.
clear ip dhcp snooping binding	Clear the dynamic user information from the DHCP snooping binding database.

9.4 Other DHCP Snooping Configuration Commands

9.4.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP snooping binding database.

clear ip dhcp snooping binding

Parameter description	N/A.

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	If users want to clear the current dynamic user information from the DHCP snooping binding database, use this command.

Examples	The following example demonstrates how to clear the dynamic database information from the DHCP snooping binding database.
	`DES-7200# clear ip dhcp snooping binding`
	`DES-7200# show ip dhcp snooping binding`
	`Total number of bindings: 0`
	`MacAddress IpAddress Lease(sec) Type VLAN Interface`
	`---------- ---------- ---------- -------- ---- ---------`

Related commands

Command	Description
show ip dhcp snooping binding	Show the information of the DHCP snooping binding database.

9.4.2 debug ip dhcp snooping

Use this command to trun on the debugging switch of the DHCP snooping.

debug ip dhcp snooping

Default	Turned off
Command mode	Privileged EXEC mode.

Examples	The following example demonstrates how to turn on the debugging switch of the DHCP snooping.
	`DES-7200# debug ip dhcp snooping`
	`DES-7200# show ip dhcp snooping binding`

9.4.3 renew ip dhcp snooping database

When the DHCP Snooping function is enabled, use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.

renew ip dhcp snooping database

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	This command is used to import the flash file information to the DHCP Snooping database in real time.
Examples	The following example demonstrates how to import the flash file information to the DHCP Snooping database. `DES-7200# renew ip dhcp snooping database`

Related commands

Command	Description
-	-

Platform description	This command is supported on all switches.

10 DAI Configuration Commands

10.1 Commands for Enabling and Disabling the DAI Inspection Function of the Specified VLAN

10.1.1 ip arp inspection vlan *vlan-id*

Use this command to enable the DAI inspection function of the specified VLAN. The **no** option of this command disables the function of the specified VLAN. If the parameter **vlan-id** is neglected, the DAI inspection function of all VLANs will be disabled.

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan [*vlan-id*]

Parameter description

Parameter	Description
vlan-id	VLAN ID

Default The DAI inspection function of all VLANs is disabled.

Command mode Global configuration mode.

Usage guidelines To execute this command, enable the DAI function firstly.

Examples The following configuration is to check the ARP message received from VLAN 1.

```
DES-7200(config)# ip arp inspection
DES-7200(config)# ip arp inspection vlan 1
```

Related

Command	Description

	show ip arp inspection vlan	Show the information of the DAI inspection function of the specified VLAN.

10.2 Commands for Configuring the L2 Port to a Trusted Port

10.2.1 ip arp inspection trust

Use this command to configure the L2 port to a trusted port.The **no** option of this command will restore the L2 port to a untrusted port.

ip arp inspection trust

no ip arp inspection trust

Default configuration	The L2 port is a untrusted port.
Command mode	Interface configuration mode.
Usage guidelines	If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.

Examples	The configuration example below sets the gigabitEthernet 0/19 interface as the trusted port.
	`DES-7200(config)# interface gigabitEthernet 0/19`
	`DES-7200(config-if)# ip arp inspection trust`

Related commands

Command	Description
show ip arp inspection interface	Show related DAI information on the interface, including the trust state and rate limit of the interface.

Platform description	On the NFPP-supported switches, interface rate is limited by NFPP rather than DAI. Therefore, if you execute this command on NFPP-supported switches, only the interface trust state will be displayed.

10.3 DHCP Snooping Database Related Configuration

When the corresponding DAI funciton of the VLAN is enabled and the L2 port which receives the ARP message is configured to be a untrusted port, the validity of the ARP message is needed to check based on the DHCP Snooping database. If no configuration is carried out for the database, the ARP message passes the validity check. For the configuration on the DHCP Snooping, refer to the *DHCP Snooping Configuration*.

11 IP Source Guard Configuration Commands

11.1 IP Source Guard Global Command

11.1.1 ip source binding

Use this command to add static user information to IP source address binding database. The **no** form of this command deletes the corresponding static user:

[**no**] **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **[interface** *interface-id* | **ip-mac** | **ip-only]**

Parameter description

Parameter	Description
mac-address	Add user MAC address statically.
vlan-id	Add user vlan id statically.
ip-address	Add user IP address statically.
interface-id	Add user interface id statically.
ip-mac	The global binding type is IP+MAC
ip-only	The global binding type is IP only.

Default configuration No static binding user.

Command mode Global configuration mode.

Examples

The following example shows how to configure a static user:

```
DES-7200# configure terminal
DES-7200(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface FastEthernet 0/1
DES-7200(config)# end
DES-7200# show ip source binding
MacAddress     IpAddress  Lease(sec)    Type      VLAN Interface
-------------- --------- ----------    ----       ---- ------------
0000.0000.0001 1.1.1.1    infinite      static      1 FastEthernet 0/1
Total number of bindings: 1
```

Related commands

Command	Description
show ip source binding	View the binding information of IP source address and database.

Platform description This command is supported on all switches.

11.2 IP Source Guard Command in the Interface Mode

11.2.1 ip verify source

Use this command to enable IP Source Guard function on the interface, The **no** form of this command disable the function.

[**no**] **ip verify source** [**port-security**]

Parameter description

Parameter	Description
port-security	Configure IP Source Guard to do IP+MAC-based detection.

Default configuration Disabled

Command mode	Interface configuration mode.
Usage guidelines	This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection. IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

Examples	The following example configures IP Source Guard on fastEthernet 0/1:
	`DES-7200# configure terminal`
	`DES-7200(config)# interface fastEthernet 0/1`
	`DES-7200(config-if)# ip verify source`
	`DES-7200(config-if)# end`

Related commands

Command	Description
show ip verify source	View user filtering entry of IP Source Guard.

Platform description	This command is supported on all switches.

11.3 Other IP Source Guard Commands

11.3.1 show ip source binding

Use this command to view the binding information of IP source address and database.

show ip binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter description

Parameter	Description
ip-address	Show user binding information of

	corresponding ip.
mac-address	Show user binding information of corresponding mac.
dhcp-snooping	Show binding information of dynamic user.
static	Show binding information of static user.
vlan-id	Show user binding information of corresponding vlan.
Interface-id	Show user binding information of corresponding interface.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show ip source binding static
MacAddress     IpAddress   Lease(sec)    Type       VLAN
Interface
-------------  ---------  ----------    ----       ----
------------
0000.0000.0001  1.0.0.1     infinite      static      1
FastEthernet 0/1
Total number of bindings: 1
```

Related commands

Command	Description
ip source binding	Set the binding static user.

Platform description

This command is supported on all switches.

11.3.2 show ip verify source

Use this command to view user filtering entry of IP Source Guard.

show ip verify source [**interface** *interface-id*]

Parameter description

Parameter	Description
Interface-id	Show user filtering entry of corresponding interface.

Command mode

Privileged EXEC mode.

Usage guidelines

If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: “IP source guard is not configured on the interface FastEthernet 0/10”

Now, IP Source Guard supports the following filtering modes:

inactive-no-snooping-vlan：the interface isn’t within the range of DHCP Snooping VLAN and IP Source Guard is inactive.

inactive-trust-port ： the interface is the trusted port controlled by DHCP Snooping and IP Source Guard is inactive.

active：the interface is the untrusted port ontrolled by DHCP Snooping and IP Source Guard is active.

Examples

```
DES-7200 # show ip verify source
Interface Filter-type Filter-mode Ip-address Mac-address   VLAN
--------- ----------- ----------- ---------- -------------- ----
FastEthernet 0/3   ip         active      3.3.3.3                   1
FastEthernet 0/3   ip         active      deny-all
FastEthernet 0/4    ip+mac     active        4.4.4.4    0000.0000.0001
1
FastEthernet 0/4   ip+mac    active       deny-all
```

Related commands

Command	Description
ip verify source	Set IP Source Guard on the

		interface.

Platform description	This command is supported on all switches.

12 NFPP Configuration Commands

12.1.1 cpu-protect sub-interface {manage | protocol | route} pps

Use this command to configure the traffic bandwidth of each type of packets.

cpu-protect sub-interface {**manage** | **protocol** | **route**} **pps** *pps_vaule*

Parameter description

Parameter	Description
pps_value	The rate limit threshold, ranging from 1 to 8192

Default

The default traffic bandwidths of each type of packets are:
Manage packets: 3000pps;
Route packets: 3000pps;
Protocol packets: 3000pps.

Command mode

Global configuration mode.

Examples

```
DES-7200(config)# cpu-protect sub-interface manage pps 200
```

Related commands

Command	Description
cpu-protect sub-interface {**manage** | **protocol** | **route**} **percent**	Configure the percent value of each type of packets occupied in the buffer area.

12.1.2 cpu-protect sub-interface {manage | protocol | route} percent

Use this command to configure the percent value of each type of packets occupied in the buffer area.

cpu-protect sub-interface {**manage** | **protocol** | **route**} **percent** *percent_vaule*

Parameter description

Parameter	Description
percent_value	The percent value, ranging from 1 to 100.

Default

The default percent values of each type of packets occupied in the buffer area are:

Manage packets: 30;

Route packets: 20;

Protocol packets: 45.

Command mode

Global configuration mode.

Examples

```
DES-7200(config)# cpu-protect sub-interface manage
percent 60
```

Related commands

Command	Description
cpu-protect sub-interface {**manage** | **protocol** | **route**} **pps**	Configure the traffic bandwidth of each type of packets.

12.2 ARP-guard Configuration Commands

The ARP-guard configuration commands include:

12.2.1 arp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack

threshold, the attack occurs.

arp-guard attack-threshold {**per-src-ip** | **per-src-mac** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the attack threshold for each source IP address.
per-src-mac	Set the attack threshold for each source MAC address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the attack threshold for each source IP address and source MAC address is 8pps; and the attack threshold for each port is 200pps.

Command mode

NFPP configuration mode.

Usage guidelines

The attack threshold shall be equal to or greater than the rate-limit threshold.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# arp-guard attack-threshold per-src-ip 2
DES-7200(config-nfpp)# arp-guard attack-threshold per-src-mac 3
DES-7200(config-nfpp)# arp-guard attack-threshold per-port 50
```

Related commands

Command	Description
nfpp arp-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard hosts	Show the monitored host.

	clear nfpp arp-guard hosts	Clear the isolated host.

12.2.2 arp-guard enable

Use this command to enable the anti-ARP guard function globally.

arp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Enabled.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# arp-guard enable
```

Related commands

Command	Description
nfpp arp-guard enable	Enable the anti-ARP attack on the interface.
show nfpp arp-guard summary	Show the configurations.

12.2.3 arp-guard isolate-period

Use this command to set the arp-guard isolate time globally.

arp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The

	valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# arp-guard isolate-period 180
```

Related commands

Command	Description
nfpp arp-guard isolate-period	Set the isolate time on the interface.
show nfpp arp-guard summary	Show the configurations.

12.2.4 arp-guard monitor-period

Use this command to configure the arp guard monitor time.

arp guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# arp-guard monitor-period 180
```

Related commands

Command	Description
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard hosts	Show the monitored host list.
clear nfpp arp-guard hosts	Clear the isolated host.

12.2.5 arp-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

arp-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines	If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.
Examples	`DES-7200(config)# nfpp` `DES-7200(config-nfpp)# arp-guard monitored-host-limit 200`

Related commands

Command	Description
show nfpp arp-guard summary	Show the configurations.

12.2.6 arp-guard rate-limit

Use this command to set the arp guard rate limit.

arp-guard rate-limit {per-src-ip | per-src-mac | per-port} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate limit for each source IP address.
per-src-mac	Set the rate limit for each source MAC address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings

The default rate limit for each source IP address and MAC address is 4pps; the default rate limit for each port is 100pps.

Command mode	NFPP configuration mode.
Usage guidelines	N/A
Examples	DES-7200(config)# **nfpp** DES-7200(config-nfpp)# **arp-guard rate-limit per-src-ip** *2* DES-7200(config-nfpp)# **arp-guard rate-limit per-src-mac** *3* DES-7200(config-nfpp)# **arp-guard rate-limit per-port** *50*

Related commands

Command	Description
nfpp arp-guard policy	Set the rate limit and the attack threshold.
show nfpp arp-guard summary	Show the configurations.

12.2.7 arp-guard scan-threshold

Use this command to set the global scan threshold.

arp-guard scan-threshold *pkt-cnt*

Parameter description

Parameter	Description
pkt-cnt	Set the scan threshold, in the range of 1-9999.

Default Settings	The default scan threshold is 15, in 10 seconds.
Command mode	NFPP configuration mode.
Usage guidelines	The scanning may occur on the condition that: more than 15 packets are received within 10 seconds; the source MAC address for the link layer is constant while the source IP address is uncertain; the source MAC and IP address for the link layer is

constant while the destination IP address is uncertain.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# arp-guard scan-threshold 20
```

Related commands

Command	Description
nfpp arp-guard scan-threshold	Set the scan threshold on the port.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard scan	Show the ARP guard scan table.
clear nfpp arp-guard scan	Clear the ARP guard scan table.

12.2.8 clear nfpp arp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp arp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
ip-address	Set the IP address.
mac-address	Set the MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command without the parameter to clear all monitored hosts.

Examples

```
DES-7200# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

Related commands	Command	Description
	arp-guard attack-threshold	Set the global attack threshold.
	nfpp arp-guard policy	Set the limit threshold and attack threshold.
	show nfpp arp-guard hosts	Show the monitored host.

12.2.9 clear nfpp arp-guard scan

Use this command to clear ARP scanning table.

clear nfpp arp-guard scan

Parameter description	Parameter	Description
	-	-

Default Settings	N/A.

Command mode	Privileged EXEC mode.

Usage guidelines	N/A.

Examples	`DES-7200# clear nfpp arp-guard scan`

Related commands	Command	Description
	arp-guard attack-threshold	Set the global attack threshold.
	nfpp arp-guard policy	Set the attack threshold.
	show nfpp arp-guard scan	Show the ARP scanning table.

12.2.10 nfpp arp-guard enable

Use this command to enable the anti-ARP attack function on the interface.

nfpp arp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The anti-ARP attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface anti-ARP attack configuration is prior to the global configuration.

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp arp-guard enable
```

Related commands

Command	Description
arp-guard enable	Enable the anti-ARP attack function.
show nfpp arp-guard summary	Show the configurations.

12.2.11 nfpp arp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp arp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.

	permanent	Permanent isolation.

Default Settings	By default, the isolate period is not configured.
Command mode	Interface configuration mode.
Usage guidelines	N/A

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp arp-guard isolate-period 180
```

Related commands

Command	Description
arp-guard isolate-period	Set the global isolate period.
show nfpp arp-guard summary	Show the configurations.

12.2.12 nfpp arp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp arp-guard policy {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate-limit threshold and the attack threshold for each source IP address.
per-src-mac	Set the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Set the rate-limit threshold and the

	attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp arp-guard policy per-src-ip 2 10
DES-7200(config-if)# nfpp arp-guard policy per-src-mac 3 10
DES-7200(config-if)# nfpp arp-guard policy per-port 50 100
```

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.
arp-guard rate-limit	Set the global rate-limit threshold.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard hosts	Show the monitored host.
clear nfpp arp-guard hosts	Clear the isolated host.

12.2.13 nfpp arp-guard scan-threshold

Use this command to set the scan threshold.

nfpp arp-guard scan-threshold *pkt-cnt*

Parameter description

Parameter	Description
pkt-cnt	Set the scan threshold with the valid range of [1, 9999].

Default Settings

By default, the sport-based scan threshold is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp arp-guard scan-threshold 20
```

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard scan	Show the ARP scan table.
clear nfpp arp-guard scan	Clear the ARP scan table.

12.3 DHCP-guard Configuration Commands

The DHCP-guard configuration commands include:

12.3.1 dhcp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

dhcp-guard attack-threshold { **per-src-mac** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the attack threshold for each source MAC address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the attack threshold for each source MAC address is 10pps; and the attack threshold for each port is 300pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)#  dhcp-guard  attack-threshold per-src-mac 15
DES-7200(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

Related commands

Command	Description
nfpp dhcp-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp dhcp-guard summary	Show the configurations.
show nfpp dhcp-guard hosts	Show the monitored host list.
clear nfpp dhcp-guard hosts	Clear the monitored host.

12.3.2 dhcp-guard enable

Use this command to enable the DHCP anti-attack function.

dhcp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcp-guard enable
```

12.3.3 dhcp-guard isolate-period

Use this command to set the isolate time globally.

dhcp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not

set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcp-guard isolate-period 180
```

Related commands

Command	Description
nfpp dhcp-guard isolate-period	Set the isolate time on the interface.
show nfpp dhcp-guard summary	Show the configurations.

12.3.4 dhcp-guard monitor-period

Use this command to configure the monitor time.

dhcp-guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcp-guard monitor-period 180
```

Related commands

Command	Description
show nfpp dhcp-guard summary	Show the configurations.
show nfpp dhcp-guard hosts	Show the monitored host list.
clear nfpp dhcp-guard hosts	Clear the isolated host.

12.3.5 dhcp-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

dhcp-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Related commands

Command	Description
show nfpp dhcp-guard summary	Show the configurations.

12.3.6 dhcp-guard rate-limit

Use this command to set the rate-limit threshold globally.

dhcp-guard rate-limit { per-src-mac | per-port} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate limit for each source MAC address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings

The default rate limit for each source MAC address is 5pps; the default rate limit for each port is 150pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
DES-7200(config-nfpp)# dhcp-guard rate-limit per-port 100
```

Related commands	Command	Description
	nfpp dhcp-guard policy	Set the rate limit and the attack threshold.
	show nfpp dhcp-guard summary	Show the configurations.

12.3.7 clear nfpp dhcp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter description	Parameter	Description
	vid	Set the VLAN ID.
	interface-id	Set the interface name and number.
	mac-address	Set the MAC address.

Default Settings	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command without the parameter to clear all monitored hosts.
Examples	`DES-7200# clear nfpp dhcp-guard hosts vlan 1 interface g0/1`

Related commands	Command	Description
	dhcp-guard attack-threshold	Set the global attack threshold.
	nfpp dhcp-guard policy	Set the limit threshold and attack threshold.
	show nfpp dhcp-guard hosts	Show the monitored host.

12.3.8 nfpp dhcp-guard enable

Use this command to enable the DHCP anti-attack function on the interface.

nfpp dhcp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The DHCP anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface DHCP anti- attack configuration is prior to the global configuration.

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp dhcp-guard enable
```

Related commands

Command	Description
dhcp-guard enable	Enable the anti-ARP attack function.
show nfpp dhcp-guard summary	Show the configurations.

12.3.9 nfpp dhcp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp dhcp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.

	permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp dhcp-guard isolate-period 180
```

Related commands

Command	Description
dhcp-guard isolate-period	Set the global isolate period.
show nfpp dhcp-guard summary	Show the configurations.

12.3.10 nfpp dhcp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp dhcp-guard policy { **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Set the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the

	valid range of [1, 9999].

Default Settings	By default, the rate-limit threshold and the attack threshold are not configured.
Command mode	Interface configuration mode.
Usage guidelines	The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples	`DES-7200(config)# interface G 0/1`
	`DES-7200(config-if)# nfpp dhcp-guard policy per-src-mac 3 10`
	`DES-7200(config-if)# nfpp dhcp-guard policy per-port 50 100`

Related commands

Command	Description
dhcp-guard attack-threshold	Set the global attack threshold.
dhcp-guard rate-limit	Set the global rate-limit threshold.
show nfpp dhcp-guard summary	Show the configurations.
show nfpp dhcp-guard hosts	Show the monitored host.
clear nfpp dhcp-guard hosts	Clear the isolated host.

12.4 DHCPv6-guard Configuration Commands

The DHCPv6-guard configuration commands include:

12.4.1 dhcpv6-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Dhcpv6-guard attack-threshold { **per-src-mac** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the attack threshold for each source MAC address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the attack threshold for each source MAC address is 10pps; and the attack threshold for each port is 300pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)#  dhcpv6-guard  attack-threshold per-src-mac 15
DES-7200(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

Related commands

Command	Description
nfpp dhcpv6-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp dhcpv6-guard summary	Show the configurations.
show nfpp dhcpv6-guard hosts	Show the monitored host list.
clear nfpp dhcpv6-guard hosts	Clear the monitored host.

12.4.2 dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function.

Dhcpv6-guard enable

Parameter description

Parameter	Description
-	-

Default Settings Disabled

Command mode NFPP configuration mode.

Usage guidelines N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcpv6-guard enable
```

12.4.3 dhcpv6-guard isolate-period

Use this command to set the isolate time globally.

dhcpv6-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings The default isolate time is 0, which means no isolation.

Command mode NFPP configuration mode.

Usage The isolate period can be configured globally or based on

guidelines	the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcpv6-guard isolate-period 180
```

Related commands

Command	Description
nfpp dhcpv6-guard isolate-period	Set the isolate time on the interface.
show nfpp dhcpv6-guard summary	Show the configurations.

12.4.4 dhcpv6-guard monitor-period

Use this command to configure the monitor time.

dhcpv6-guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the

attackers on the interface will be removed rather than being monitored by the software.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcpv6-guard monitor-period 180
```

Related commands

Command	Description
show nfpp dhcpv6-guard summary	Show the configurations.
show nfpp dhcpv6-guard hosts	Show the monitored host list.
clear nfpp dhcpv6-guard hosts	Clear the isolated host.

12.4.5 dhcpv6-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

dhcpv6-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcpv6-guard monitored-host-limit 200
```

Related commands

Command	Description
show nfpp dhcpv6-guard summary	Show the configurations.

12.4.6 dhcpv6-guard rate-limit

Use this command to set the rate-limit threshold globally.

dhcpv6-guard rate-limit { per-src-mac | per-port} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate limit for each source MAC address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings

The default rate limit for each source MAC address is 5pps; the default rate limit for each port is 150pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
```

```
DES-7200(config-nfpp)# dhcpv6-guard rate-limit per-port 100
```

Related commands

Command	Description
nfpp dhcpv6-guard policy	Set the rate limit and the attack threshold.
show nfpp dhcpv6-guard summary	Show the configurations.

12.4.7 clear nfpp dhcpv6-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp dhcpv6-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
mac-address	Set the MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command without the parameter to clear all monitored hosts.

Examples

```
DES-7200# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

Related commands

Command	Description
dhcpv6-guard attack-threshold	Set the global attack threshold.

nfpp dhcpv6-guard policy	Set the limit threshold and attack threshold.
show nfpp dhcpv6-guard hosts	Show the monitored host.

12.4.8 nfpp dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function on the interface.

nfpp dhcpv6-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The DHCPv6 anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface DHCPv6 anti- attack configuration is prior to the global configuration.

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp dhcpv6-guard enable
```

Related commands

Command	Description
dhcpv6-guard enable	Enable the anti-ARP attack function.
show nfpp dhcpv6-guard summary	Show the configurations.

12.4.9 nfpp dhcpv6-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp dhcpv6-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp dhcpv6-guard isolate-period
180
```

Related commands

Command	Description
dhcpv6-guard isolate-period	Set the global isolate period.
show nfpp dhcpv6-guard summary	Show the configurations.

12.4.10 nfpp dhcpv6-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp dhcpv6-guard policy { **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate-limit threshold and the attack threshold for each source MAC address.

per-port	Set the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
DES-7200(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related commands

Command	Description
dhcpv6-guard attack-threshold	Set the global attack threshold.
dhcpv6-guard rate-limit	Set the global rate-limit threshold.
show nfpp dhcpv6-guard summary	Show the configurations.
show nfpp dhcpv6-guard hosts	Show the monitored host.
clear nfpp dhcpv6-guard hosts	Clear the isolated host.

12.5 ICMP-guard Configuration Commands

The ICMP-guard configuration commands include:

12.5.1 icmp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

icmp-guard attack-threshold { **per-src-ip** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the attack threshold for each source IP address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the attack threshold and the rate-limit threshold for each source IP address and each port are the same. For the default rate-limit threshold value, see the **icmp-guard rate-limit** command.

Command mode

NFPP configuration mode.

Usage guidelines

N/A.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)#  icmp-guard  attack-threshold per-src-ip 600
DES-7200(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

Related commands

Command	Description
nfpp icmp-guard policy	Show the rate-limit threshold and attack threshold.

show nfpp icmp-guard summary	Show the configurations.
show nfpp icmp-guard hosts	Show the monitored host list.
clear nfpp icmp-guard hosts	Clear the monitored host.

12.5.2 icmp-guard enable

Use this command to enable the ICMP anti-attack function.

icmp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Enabled

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# icmp-guard enable
```

Related commands

Command	Description
nffp icmp-guard enable	Enable the ICMP anti-attack function on the interface.
show nfpp icmp-guard summary	Show the configurations.

12.5.3 icmp-guard isolate-period

Use this command to set the isolate time globally.

icmp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# icmp-guard isolate-period 180
```

Related commands

Command	Description
nfpp icmp-guard isolate-period	Set the isolate time on the interface.
show nfpp icmp-guard summary	Show the configurations.

12.5.4 icmp-guard monitor-period

Use this command to configure the monitor time.

icmp-guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings	600s
Command mode	NFPP configuration mode.
Usage guidelines	When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.
Examples	`DES-7200(config)# nfpp` `DES-7200(config-nfpp)# icmp-guard monitor-period 180`

Related commands

Command	Description
show nfpp icmp-guard summary	Show the configurations.
show nfpp icmp-guard hosts	Show the monitored host list.
clear nfpp icmp-guard hosts	Clear the isolated host.

12.5.5 icmp-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

icmp-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings	1000
Command mode	NFPP configuration mode
Usage guidelines	If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.
Examples	`DES-7200(config)# nfpp` `DES-7200(config-nfpp)# icmp-guard monitored-host-limit 200`

Related commands

Command	Description
show nfpp icmp-guard summary	Show the configurations.

12.5.6 icmp-guard rate-limit

Use this command to set the rate-limit threshold globally.

icmp-guard rate-limit { per-src-ip | per-port} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate limit for each source IP address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings	The default rate-limit threshold for each source IP address is half of the value for each port. The default rate-limit threshold value for each port varies with the products.
Command mode	NFPP configuration mode.
Usage guidelines	N/A

Examples	`DES-7200(config)# nfpp`
	`DES-7200(config-nfpp)# icmp-guard rate-limit per-src-ip 500`
	`DES-7200(config-nfpp)# icmp-guard rate-limit per-port 800`

Related commands

Command	Description
nfpp icmp-guard policy	Set the rate limit and the attack threshold.
show nfpp icmp-guard summary	Show the configurations.

12.5.7 icmp-guard trusted-host

Use this command to set the trusted hosts free form monitoring.

icmp-guard trusted-host *ip mask*

no icmp-guard trusted-host {**all |** *ip mask*}

Parameter description

Parameter	Description
ip	Set the IP address.
mask	Set the IP mask.
all	Delete the configurations of all trusted hosts.

Default Settings	N/A.

Command mode	NFPP configuration mode.
Usage guidelines	The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.
Examples	`DES-7200(config)# nfpp` `DES-7200(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0`

Related commands

Command	Description
show nfpp icmp-guard trusted-host	Show the configurations.

12.5.8 clear nfpp icmp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
ip-address	Set the IP address.

Default Settings	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command without the parameter to clear all monitored hosts.

Examples

```
DES-7200# clear nfpp icmp-guard hosts vlan 1 interface
g0/1
```

Related commands

Command	Description
icmp-guard attack-threshold	Set the global attack threshold.
nfpp icmp-guard policy	Set the limit threshold and attack threshold.
show nfpp icmp-guard hosts	Show the monitored host.

12.5.9 nfpp icmp-guard enable

Use this command to enable the ICMP anti-attack function on the interface.

nfpp icmp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The ICMP anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface ICMP anti- attack configuration is prior to the global configuration.

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp icmp-guard enable
```

Related commands

Command	Description
icmp-guard enable	Enable the anti-ARP attack function.

	show nfpp icmp-guard summary	Show the configurations.

12.5.10 nfpp icmp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp icmp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp icmp-guard isolate-period 180
```

Related commands

Command	Description
icmp-guard isolate-period	Set the global isolate period.
show nfpp icmp-guard summary	Show the configurations.

12.5.11 nfpp icmp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp icmp-guard policy { **per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate-limit threshold and the attack threshold for each source IP address.
per-port	Set the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp icmp-guard policy per-src-ip 5 10
DES-7200(config-if)# nfpp icmp-guard policy per-port 100 200
```

Related commands

Command	Description
icmp-guard attack-threshold	Set the global attack threshold.
icmp-guard rate-limit	Set the global rate-limit threshold.

show nfpp icmp-guard summary	Show the configurations.
show nfpp icmp-guard hosts	Show the monitored host.
clear nfpp icmp-guard hosts	Clear the isolated host.

12.6 IP-guard Configuration Commands

The IP-guard configuration commands include:

Caution	It is worth mentioning that ip-guard is for the attack of the IP packets whose destination IP address is not the local one. CPP(CPU Protect Policy) limits the rate of the IP packets whose destination IP address is the local one. IP-guard is not supported for the layer 2 switches and only supported for the layer 3 switches.

12.6.1 ip-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

ip-guard attack-threshold { **per-src-ip** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the attack threshold for each source IP address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings	By default, the attack threshold for each source IP address and each port are 20pps and 2000pps respectively.
Command mode	NFPP configuration mode.
Usage	The attack threshold shall be equal to or larger than the

guidelines	rate-limit threshold.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)#    ip-guard    attack-threshold
per-src-ip 2
DES-7200(config-nfpp)# ip-guard attack-threshold
per-port 50
```

Related commands

Command	Description
nfpp ip-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Show the configurations.
show nfpp ip-guard hosts	Show the monitored host list.
clear nfpp ip-guard hosts	Clear the monitored host.

12.6.2 ip-guard enable

Use this command to enable the IP anti-scanfunction.

ip-guard enable

Parameter description

Parameter	Description
-	-

Default Settings	Enabled
Command mode	NFPP configuration mode.
Usage guidelines	N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# ip-guard enable
```

Related commands

Command	Description
nffp ip-guard enable	Enable the IP anti-scan function on the interface.

12.6.3 ip-guard isolate-period

Use this command to set the isolate time globally.

ip-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

N/A.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# ip-guard isolate-period 180
```

Related commands

Command	Description
nfpp ip-guard isolate-period	Set the isolate time on the interface.
show nfpp ip-guard summary	Show the configurations.

12.6.4 ip-guard monitor-period

Use this command to configure the monitor time.

ip-guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# ip-guard monitor-period 180
```

Related commands

Command	Description
show nfpp ip-guard summary	Show the configurations.
show nfpp ip-guard hosts	Show the monitored host list.
clear nfpp ip-guard hosts	Clear the isolated host.

12.6.5 ip-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

ip-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# ip-guard monitored-host-limit 200
```

Related commands

Command	Description
show nfpp ip-guard summary	Show the configurations.

12.6.6 ip-guard rate-limit

Use this command to set the rate-limit threshold globally.

ip-guard rate-limit { per-src-ip | per-port} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate limit for each source IP

	address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings By default, the the rate-limit threshold for each source IP address and each port is 20pps and 100pps respectively.

Command mode NFPP configuration mode.

Usage guidelines N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# ip-guard rate-limit per-src-ip 2
DES-7200(config-nfpp)# ip-guard rate-limit per-port 50
```

Related commands

Command	Description
nfpp ip-guard policy	Set the rate limit and the attack threshold.
show nfpp ip-guard summary	Show the configurations.

12.6.7 ip-guard scan-threshold

Use this command to set the global scan threshold.

ip-guard scan-threshold *pkt-cnt*

Parameter description

Parameter	Description
pkt-cnt	Set the scan threshold, in the range of 1-9999.

Default Settings The default scan threshold is 100, in 10 seconds.

Command mode	NFPP configuration mode.
Usage guidelines	N/A.
Examples	`DES-7200(config)# nfpp` `DES-7200(config-nfpp)# ip-guard scan-threshold 20`

Related commands

Command	Description
nfpp ip-guard scan-threshold	Set the scan threshold on the port.
show nfpp ip-guard summary	Show the configurations.

12.6.8 ip-guard trusted-host

Use this command to set the trusted hosts free form monitoring.

ip-guard trusted-host *ip mask*

no ip-guard trusted-host {**all |** *ip mask*}

Parameter description

Parameter	Description
ip	Set the IP address.
mask	Set the IP mask.
all	Delete the configurations of all trusted hosts.

Default Settings	N/A.
Command mode	NFPP configuration mode.
Usage guidelines	The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts

	in one network segment free from monitoring. UP to 500 trusted hosts are supported.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# ip-guard trusted-host 1.1.1.0
255.255.255.0
```

Related commands

Command	Description
show nfpp ip-guard trusted-host	Show the configurations.

12.6.9 clear nfpp ip-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp ip-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
ip-address	Set the IP address.

Default Settings N/A.

Command mode Privileged EXEC mode.

Usage guidelines Use this command without the parameter to clear all monitored hosts.

Examples

```
DES-7200# clear nfpp ip-guard hosts vlan 1 interface g0/1
```

Related commands

Command	Description
ip-guard attack-threshold	Set the global attack threshold.

	nfpp ip-guard policy	Set the limit threshold and attack threshold.
	show nfpp ip-guard hosts	Show the monitored host.

12.6.10 nfpp ip-guard enable

Use this command to enable the ICMP anti-attack function on the interface.

nfpp ip-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The IP anti-scan function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface IP anti-scan configuration is prior to the global configuration.

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp ip-guard enable
```

Related commands

Command	Description
ip-guard enable	Enable the anti-ARP attack function.
show nfpp ip-guard summary	Show the configurations.

12.6.11 nfpp ip-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp ip-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp ip-guard isolate-period 180
```

Related commands

Command	Description
ip-guard isolate-period	Set the global isolate period.
show nfpp ip-guard summary	Show the configurations.

12.6.12 nfpp ip-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp ip-guard policy { **per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate-limit threshold and the attack threshold for each source IP address.
per-port	Set the rate-limit threshold and the attack threshold for each port.

	rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
	attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings By default, the rate-limit threshold and the attack threshold are not configured.

Command mode Interface configuration mode.

Usage guidelines The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp ip-guard policy per-src-ip 2 10
DES-7200(config-if)# nfpp ip-guard policy per-port 50 100
```

Related commands

Command	Description
ip-guard attack-threshold	Set the global attack threshold.
ip-guard rate-limit	Set the global rate-limit threshold.
show nfpp ip-guard summary	Show the configurations.
show nfpp ip-guard hosts	Show the monitored host.
clear nfpp ip-guard hosts	Clear the isolated host.

12.6.13 nfpp ip-guard scan-threshold

Use this command to set the scan threshold.

nfpp ip-guard scan-threshold *pkt-cnt*

Parameter description

Parameter	Description
pkt-cnt	Set the scan threshold with the valid

		range of [1, 9999].

Default Settings	By default, the sport-based scan threshold is not configured.
Command mode	Interface configuration mode.
Usage guidelines	N/A
Examples	`DES-7200(config)# interface G 0/1` `DES-7200(config-if)# nfpp ip-guard scan-threshold 20`

Related commands

Command	Description
ip-guard attack-threshold	Set the global attack threshold.
show nfpp ip-guard summary	Show the configurations.

12.7 ND-guard Configuration Commands

The ND-guard configuration commands include:

12.7.1 nd-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

nd-guard attack-threshold per-port{ **ns-na** | **rs | ra-redirect** } *pps*

Parameter description

Parameter	Description
ns-na	Set the neighbor request and neighbor advertisement.
rs	Set the router request.
ra-redirect	Set the router advertisement and the redirect packets.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings	By default, the default attack threshold for the ns-na, rs and ra-redirect on each port is 30.
Command mode	NFPP configuration mode.
Usage guidelines	The attack threshold shall be equal to or larger than the rate-limit threshold.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
DES-7200(config-nfpp)# nd-guard attack-threshold per-port rs 10
DES-7200(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
```

Related commands

Command	Description
nfpp ip-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Show the configurations.

12.7.2 nd-guard enable

Use this command to enable the ND anti-attack function.

nd-guard enable

Parameter description

Parameter	Description
-	-

Default Settings	Enabled
Command mode	NFPP configuration mode.

Usage guidelines	N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nd-guard enable
```

Related commands

Command	Description
nffp nd-guard enable	Enable the ND anti-attack function on the interface.
show nfpp nd-guard summary	Show the configurations.

12.7.3 nd-guard rate-limit

Use this command to set the rate-limit threshold globally.

nd-guard rate-limit per-port {**ns-na** | **rs** | **ra-redirect**} *pps*

Parameter description

Parameter	Description
ns-na	Set the neighbor request and neighbor advertisement.
rs	Set the router request.
ra-redirect	Set the router advertisement and the redirect packets.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings	By default, the default rate-limit threshold for the ns-na, rs and ra-redirect on each port is 15.
Command mode	NFPP configuration mode.
Usage guidelines	N/A

Examples

```
DES-7200(config)# nfpp
```

```
DES-7200(config-nfpp)# nd-guard rate-limit per-port ns
-na 10
DES-7200(config-nfpp)# nd-guard rate-limit per-port rs
 5
DES-7200(config-nfpp)#  nd-guard  rate-limit  per-port
ra-redirect 5
```

Related commands

Command	Description
nfpp nd-guard policy	Set the rate limit and the attack threshold.
show nfpp nd-guard summary	Show the configurations.

12.7.4 nfpp nd-guard enable

Use this command to enable the ND anti-attack function on the interface.

nfpp nd-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The ND anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface ND anti-attack configuration is prior to the global configuration.

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp nd-guard enable
```

Related commands

Command	Description
nd-guard enable	Enable the ND anti- attack function.

	show nfpp nd-guard summary	Show the configurations.

12.7.5 nfpp nd-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp nd-guard policy per-port {**ns-na** | **rs** | **ra-redirect**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
ns-na	Set the neighbor request and neighbor advertisement.
rs	Set the router request.
ra-redirect	Set the router advertisement and the redirect packets.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

For ND snooping, the port is classified into untrusted port and trusted port. The untrusted port connects to the host and the trusted port connects to the gateway. The rate-limt threshold for the trusted port shall higher than the one for the untrusted port because the traffic of the trusted port generally is higher than the traffic of the untrusted port. For the trusted port with ND snooping enabled, ND snooping advertises ND guard to set the rate-limit threshold and attack threshold for the three categories of

packets as 800pps and 900pps respectively.

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp nd-guard policy per-port ns-na 50 100
DES-7200(config-if)# nfpp nd-guard policy per-port rs 10 20
DES-7200(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

Related commands

Command	Description
nd-guard attack-threshold	Set the global attack threshold.
nd-guard rate-limit	Set the global rate-limit threshold.
show nfpp nd-guard summary	Show the configurations.

12.8 Defined-guard Configuration Commands

The defined-guard configuration commands include:

12.8.1 clear nfpp define *name* hosts

Use this command to clear the monitored hosts. If the host is isolated, you need to disisolate it.

clear nfpp define *name* **hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]

Parameter description

Parameter	Description
name	Defined guard name
vid	VLAN ID
interface-id	Interface name
ip-address	IP address
ipv6-address	IPv6 address

Default Settings	N/A
Command mode	Privileged mode.
Usage guidelines	Use this command without the parameter to clear all monitored hosts.
Examples	`DES-7200# clear nfpp define tcp hosts vlan 1 interface g 0/1`

Related commands

Command	Description
show nfpp define hosts	Show the isolated hosts.

12.8.2 define *name* enable

Use this command to enable the user-defined anti-attack globally.

define *name* **enable**

Parameter description

Parameter	Description
name	Define guard name

Default Settings	N/A
Command mode	NFPP configuration mode.
Usage guidelines	This command takes effect only after the match, rate-out, rate-limit and attack-threshold have been configured.
Examples	`DES-7200(config)# nfpp` `DES-7200(config-nfpp)#define tcp enable`

Related

Command	Description

	show nfpp define summary	Show the user-defined anti-attack configurations

12.8.3 isolate-period

Use this command to set the isolate time.

isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0 or [30, 86400]. 0 for no isolation.
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP define configuration mode.

Usage guidelines

If the isolate time is not 0, the host with the packets rate exceeding the attack threshold will be isolated and the packets sent by this host will be discarded.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nfpp define tcp
DES-7200(config-nfpp-define)#isolate-period permanent
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

12.8.4 match

Use this command to specify the message matching filed for the user-defined anti-attack.

match [etype *type***] [src-mac** *smac* **[src-mac-mask** *smac_mask***]] [dst-mac** *dmac*

[dst-mac-mask *dst_mask***]] [protocol** *protocol***] [src-ip** *sip* **[src-ip-mask** *sip-mask***]] [src-ipv6** *sipv6* **[src-ipv6-masklen** *sipv6-masklen***]] [dst-ip** *dip* **[dst-ip-mask** *dip-mask***]] [dst-ipv6** *dipv6* **[dst-ipv6-masklen** *dipv6-masklen***]][src-port** *sport***] [dst-port** *dport***]**

Parameter description

Parameter	Description
type	Ethernet link layer packet type
smac	Source MAC address
smac_mask	Source MAC address mask
dmac	Destination MAC address
dmac_mask	Destination MAC address mask
protocol	IPv4/v6 message protocol
sip	Source IPv4 address
sip_mask	Source IPv4 address mask
sipv6	Source IPv6 address
sipv6_masklen	Source IPv6 address mask
dip	Destination IPv4 address
dip_mask	Destination IPv4 address mask
dipv6	Destination IPv6 address
dipv6_masklen	Length of the destination IPv6 address mask.
sport	Source port
dport	Destination port

Default Settings N/A

Command mode NFPP configuration mode.

Usage Use this command to create a new user-defined

guidelines	anti-attack type and specify the message fileds to be matched.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nfpp define tcp
DES-7200(config-nfpp-define)#match etype 0x0800 protocol 0x06
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

12.8.5 monitored-host-limit

Use this command to set the maxmum monitored host number.

monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings	1000
Command mode	NFPP define configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% % NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 1000 monitored hosts.` to remind the administrator.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nfpp define tcp
DES-7200(config-nfpp-define)#monitored-host-limit 500
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

12.8.6 monitor period

Use this command to set the monitoring time.

monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP define configuration mode.

Usage guidelines

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nfpp define tcp
DES-7200(config-nfpp-define)#monitor-period 1000
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

12.8.7 nfpp define

Use this command to create the user-defined anti-attack type.

nfpp define *name*

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.

Default Settings

N/A

Command mode

NFPP configuration mode.

Usage guidelines

Use this command to create a new user-defined anti-attack type.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nfpp define tcp
DES-7200(config-nfpp-define)#
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

12.8.8 trusted-host

Use this command to set the trusted hosts free form monitoring.

trusted-host {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}

no trusted-host {**all |** *ip mask* | *IPv6/prefixlen* }

Parameter description

Parameter	Description
ip	Set the IP address.
mac	MAC address.
mac_mask	MAC address mask.
IPv6/prefixlen	IPv6 address and mask length
mask	IP mask.
all	Delete the configurations of all trusted hosts with the **no** form of this command.

Default Settings

N/A.

Command mode

NFPP define configuration mode.

Usage guidelines

The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring.

UP to 500 trusted hosts are supported.

Before configuring the trusted-host, the match type must be configured. If the message type configured by the match is Ipv4, the Ipv6 trusted addresses are not allowed. In the same way, if the message type is IPv6, the IPv4 trusted addresses are not allowed.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# define tcp
DES-7200(config-nfpp-define)#trusted-host      1.1.1.1
255.255.255.255
```

Related

Command	Description

	show nfpp define trusted-host	Show the trusted host configurations.

12.8.9 global-policy

Use this command to set the rate-limit threshold and attack threshold based on the host or port.

global-policy {per-src-mac | per-src-ip | per-port} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Perform the rate statistics based on the source IP / VID and port.
per-src-mac	Perform the rate statistics based on the source MAC / VID and port.
per-port	Perform the rate statistics based on each physical port of receiving the packets.
rate-limit-pps	Set the rate-limit threshold.
attack-threshold-pps	Set the attack threshold.

Default Settings

N/A.

Command mode

NFPP define configuration mode.

Usage guidelines

To create a user-defined anti-attack type, the classification rule for the rate statistics must be specified, that is, recognize the host based on the source IP address/ source MAC address for the user-defined packets rate statistics based on the user / port and specify the rate-limit threshold and attack threshold for each classification. The rate-limit threshold shall be equal to or greater than the attack threshold. If the rate is greater than the rate-limit threshold, the packets that meet this classification rule will be discarded. If the rate exceeds the attack threshold, the user will be regarded as an attacker. The log will be printed and the trap will be sent. For the classification

based on the user, the user will be isolated according to the isolate period.

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# nfpp define tcp
DES-7200(config-nfpp-define)# global-policy per-src-ip 10 20
DES-7200(config-nfpp-define)# global-policy per-port 100 200
```

Related commands

Command	Description
nfpp define *name* **policy**	Set the rate-limit threshold and attack threshold.
show nfpp define summary	Show the user-defined anti-attack configurations

12.8.10 nfpp define *name* enable

Use this command to enable the user-defined anti-attack function on the interface.

nfpp define *name* **enable**

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type

Default Settings

N/A

Command mode

Interface configuration mode.

Usage guidelines

This command takes effect only after the name of the user-defined anti-attack and the match, rate-count, rate-limit and the attack-threshold have been configured.

Examples

```
DES-7200(config)# interface G0/1
DES-7200(config-if)# nfpp define tcp enable
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

12.8.11 nfpp define *name* isolate-period

Use this command to set the local isolate period in the interface configuration mode.

nfpp define *name* **isolate-period** {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
name	Name of the user-defined anti-attack type.
permanent	Permanent isolation.

Default Settings

By default, the local isolate period is not configured. The global isolate period is used.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp define tcp isolate-period 180
```

Related commands

Command	Description
isolate-period	Set the global isolate period.
show nfpp define summary	Show the configurations.

12.8.12 nfpp define *name* policy

Use this command to set the local rate-limit threshold and the attack threshold.

nfpp define *name* **policy** {**per-src-ip | per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Set the attack threshold for each source IP address.
per-port	Set the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
DES-7200(config)# interface G 0/1
DES-7200(config-if)# nfpp define tcp policy per-src-ip 2 10
DES-7200(config-if)# nfpp define tcp policy per-port 50 100
```

Related commands

Command	Description
define-policy	Set the global rate-limit threshold and attack threshold.

	show nfpp define summary	Show the user-defined anti-attack configurations.

12.9 NFPP Log Configuration Commands

The NFPP log configuration commands include:

12.9.1 clear nfpp log

Use this command to clear the NFPP log buffer area.

clear nfpp log

Parameter description

Parameter	Description
-	-

Default Settings N/A

Command mode Privileged EXEC mode.

Usage guidelines N/A

Examples

```
DES-7200# clear nfpp log
32 log-buffer entries were cleared.
```

Related commands

Command	Description
show nfpp log	Show the NFPP log configurations or the log buffer area.

12.9.2 log-buffer entries

Use this command to set the NFPP log buffer area size.

log-buffer entries *number*

Parameter description

Parameter	Description
number	The buffer area size. The valid range is [0, 1024].

Default Settings

256.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# log-buffer entries 50
```

Related commands

Command	Description
log-buffer logs *number_of_message* **interval** *length_in_seconds*	Show the rate of the syslog generated from the NFPP buffer area.
show nfpp log	Show the NFPP log configuration or the log buffer area.

12.9.3 log-buffer logs

Use this command to set the rate of syslog generated from the NFPP log buffer area.

log-buffer logs *number_of_message* **interval** *length_in_seconds*

Parameter description

Parameter	Description
number_of_message	The valid range is 0-1024. 0 indicates that all logs are recorded in the specific buffer area and no syslogs are generated.
length_in_seconds	The valid range is 0-86400(one day). 0 indicates not to write the log to the buffer area but generate the syslog immediately. With both the *number_of_message* and *length_in_seconds* values are 0, it indicates not to write the log to the buffer area but generate the syslog immediately. The parameter *number_of_message /length_in_second* indicates the rate of syslog generated from the NFPP log buffer area.

Default Settings

By default, the *number_of_message is* 1 and the *length_in_seconds* is 30.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# log-buffer logs 2 interval 12
```

Related

Command	Description

log-buffer entries *number*	Set the NFPP log buffer area size.
show nfpp log summary	Show the NFPP log configurations or the log buffer area.

12.9.4 logging

Use this command to set the VLAN or the interface log for NFPP.

logging vlan *vlan-range*

logging interface *interface-id*

Parameter description

Parameter	Description
vlan-range	Set the specified VLAN range, in the format such as “1-3, 5”.
interface-id	Set the interface ID.

Default Settings

All logs are recorded..

Command mode

NFPP configuration mode.

Usage guidelines

Use this command to filter the logs and records the logs within the specified VLAN range or the specified port.

Examples

The following example shows the administrator how to record the logs in VLAN 1、VLAN 2、VLAN 3 and VLAN 5 only:

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# logging vlan 1-3,5
```

The following example shows the administrator how to record the logs on the interface GigabitEthernet 0/1 only:

```
DES-7200(config)# nfpp
DES-7200(config-nfpp)# logging interface G 0/1
```

Related commands

Command	Description
show nfpp log summary	Show the NFPP log configurations or the log buffer area.

12.9.5 show nfpp log

Use this command to show the NFPP log configuration.

show nfpp log summary

Use this command to show the NFPP log buffer area content.

show nfpp log buffer [**statistics**]

Parameter description

Parameter	Description
statistics	Show the statistical information of the NFPP log buffer area.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

When the log buffer area is full, the subsequent logs are to be dropped, and an entry with all attributes "-" is displayed in the log buffer area. The administrator shall increase the capacity of the log buffer area or improve the rate of generating the syslog.

The generated syslog in the log buffer area carries with the timestamp, for example:

```
%NFPP_ARP_GUARD-4-DOS_DETECTED:
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was
detected.(2009-07-01 13:00:00)
```

Examples

The following example shows the NFPP log configurations:

```
DES-7200#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
```

```
Logging:
  VLAN  1-3, 5
  interface Gi 0/1
  interface Gi 0/2
```

The following example shows the log number in the buffer area:

```
DES-7200#show nfpp log buffer statistics
There are 6 logs in buffer.
```

The following example shows the NFPP log buffer area:

```
DES-7200#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address    Reas
on         Timestamp
------- ----  --------   ---------  -----------    ----
--         ---------
ARP    1     Gi0/1      1.1.1.1     -      DoS
   2009-05-30 16:23:10
ARP    1     Gi0/1      1.1.1.1     -      ISOLATED
   2009-05-30 16:23:10
ARP    1     Gi0/1      1.1.1.2     -       DoS
    2009-05-30 16:23:15
ARP    1     Gi0/1      1.1.1.2     -       ISOLATE_FAI
LED 2009-05-30 16:23:15
ARP    1     Gi0/1      -         0000.0000.0001  SCAN
         2009-05-30 16:30:10
ARP    -     Gi0/2      -         -          PORT_ATTACK
ED   2009-05-30 16:30:10
```

Field	Description
Protocol	ARP，IP，ICMP，DHCP，DHCPv6，NS-NA，RS，RA-REDIRECT
Reason	1. DoS 2. ISOLATED 3. ISOLATE_FAILE 4. SCAN 5. PORT_ATTACKED

Related commands

Command	Description
clear nfpp log	Clear the NFPP log buffer area.

12.10 ARP-guard Showing Related Commands

12.10.1 show nfpp arp-guard hosts

Use this command to show the monitored host.

show nfpp arp-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
DES-7200# show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example shows the monitored host:

```
DES-7200# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate
user" .
VLAN  interface IP address   MAC address   remain-time(s)
----  --------   ---------   -----------
-------------
1     Gi0/1      1.1.1.1     -               110
2     Gi0/2      1.1.2.1     -               61
*3    Gi0/3      -           0000.0000.1111  110
4     Gi0/4      -           0000.0000.2222   61
Total：4 hosts
```

Related commands

Command	Description
clear nfpp arp-guard hosts	Clear the monitored host.

12.10.2 show nfpp arp-guard scan

Use this command to show the ARP scan list.

show nfpp arp-guard scan [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the ARP scan list.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp arp-guard scan statistics
ARP scan table has 4 record(s).


DES-7200# show nfpp arp-guard scan
VLAN    interface   IP address   MAC address    timestamp
----    --------   ----------  -----------    ---------
1       Gi0/1      N/A          0000.0000.0001
2008-01-23 16:23:10
2       Gi0/2      1.1.1.1      0000.0000.0002
2008-01-23 16:24:10
3       Gi0/3      N/A          0000.0000.0003
2008-01-23 16:25:10
4       Gi0/4      N/A          0000.0000.0004
2008-01-23 16:26:10
Total：4 record(s)


DES-7200# show nfpp arp-guard scan vlan 1 interface G 0/1
0000.0000.0001
VLAN    interface   IP address   MAC address    timestamp
----    --------    ----------    -----------    -------
1       Gi0/1      N/A           0000.0000.0001
2008-01-23 16:23:10
Total：1 record(s)
```

Related commands

Command	Description
arp-guard scan-threshold	Set the global scan threshold.
nfpp arp-guard scan-threshold	Set the scan threshold.
clear nfpp arp-guard scan	Clear the ARP scan list.

12.10.3 show nfpp arp-guard summary

Use this command to show the configurations.

show nfpp arp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp arp-guard summary
（Format of column Rate-limit and  Attack-threshold is p
er-src-ip/per-src-mac/per-port.）
Interface  Status  Isolate-period Rate-limit Attack-thr
eshold Scan-threshold
Global     Enable  300            4/5/60    8/10/100
       15
Gi 0/1      Enable  180            5/-/-      8/-/-
         -
Gi 0/2      Disable 200            4/5/60    8/10/100
        20

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.
arp-guard enable	Enable the anti-ARP attack function.
arp-guard isolate-period	Set the global isolate time.
arp-guard monitor-period	Set the monitor period.
arp-guard monitored-host-limit	Set the maximum number of the monitored hosts.
arp-guard rate-limit	Set the global rate-limit threshold.
arp-guard scan-threshold	Set the global scan threshold.
nfpp arp-guard enable	Enable the anti-ARP attack function on the interface.
nfpp arp-guard isolate-period	Set the isolate time.
nfpp arp-guard policy	Set the rate-limit threshold and attack threshold.
nfpp arp-guard scan-threshold	Set the scan threshold.

12.11 DHCP-guard Showing Related Commands

12.11.1 show nfpp dhcp-guard hosts

Use this command to show the monitored host.

show nfpp dhcp-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.

vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
DES-7200# show nfpp dhcp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example shows the monitored host:

```
DES-7200# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate
host".
VLAN  interface   MAC address    remain-time(seconds)
----    ---------    -----------
-------------------
 1    gi0/2     0000.0000.0001   10
 *2   gi0/1     0000.0000.0002   20
Total: 2 host(s)
```

Related commands

Command	Description
clear nfpp dhcp-guard hosts	Clear the monitored host.

12.11.2 show nfpp dhcp-guard summary

Use this command to show the configurations.

show nfpp dhcp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp dhcp-guard summary
（Format of column Rate-limit and  Attack-threshold is p
er-src-ip/per-src-mac/per-port.）
Interface      Status      Isolate-period   Rate-limit
Attack-threshold
Global     Enable  300            -/5/150     -/10/300
Gi 0/1      Enable  180            -/6/-       -/8/-
Gi 0/2      Disable 200            -/5/30      -/10/50

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

-	No configuration.

Related commands

Command	Description
dhcp-guard attack-threshold	Set the global attack threshold.
dhcp-guard enable	Enable the DHCP anti-attack function.
dhcp-guard isolate-period	Set the global isolate time.
dhcp-guard monitor-period	Set the monitor period.
dhcp-guard monitored-host-limit	Set the maximum number of the monitored hosts.
dhcp-guard rate-limit	Set the global rate-limit threshold.
nfpp dhcp-guard enable	Enable the DHCP anti-attack function on the interface.
nfpp dhcp-guard isolate-period	Set the isolate time.
nfpp dhcp-guard policy	Set the rate-limit threshold and attack threshold.

12.12 DHCPv6-guard Showing Related Commands

12.12.1 show nfpp dhcpv6-guard hosts

Use this command to show the monitored host.

show nfpp dhcpv6-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.

interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
DES-7200# show nfpp dhcpv6-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example shows the monitored host:

```
DES-7200# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate
host".
VLAN  interface   MAC address    remain-time(seconds)
----    ---------    -----------
-------------------
 1    gi0/2     0000.0000.0001   10
 *2   gi0/1     0000.0000.0002   20
Total: 2 host(s)
```

Related commands

Command	Description
clear nfpp dhcpv6-guard hosts	Clear the monitored host.

12.12.2 show nfpp dhcpv6-guard summary

Use this command to show the configurations.

show nfpp dhcpv6-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp dhcpv6-guard summary
（Format of column Rate-limit and  Attack-threshold is p
er-src-ip/per-src-mac/per-port.）
Interface      Status      Isolate-period   Rate-limit
Attack-threshold
Global     Enable  300            -/5/150     -/10/300
Gi 0/1      Enable  180            -/6/-       -/8/-
Gi 0/2      Disable 200            -/5/30      -/10/50

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

-	No configuration.

Related commands

Command	Description
dhcpv6-guard attack-threshold	Set the global attack threshold.
dhcpv6-guard enable	Enable the DHCPv6 anti-attack function.
dhcpv6-guard isolate-period	Set the global isolate time.
dhcpv6-guard monitor-period	Set the monitor period.
dhcpv6-guard monitored-host-limit	Set the maximum number of the monitored hosts.
dhcpv6-guard rate-limit	Set the global rate-limit threshold.
nfpp dhcpv6-guard enable	Enable the DHCPv6 anti-attack function on the interface.
nfpp dhcpv6-guard isolate-period	Set the isolate time.
nfpp dhcpv6-guard policy	Set the rate-limit threshold and attack threshold.

12.13 ICMP-guard Showing Related Commands

12.13.1 show nfpp icmp-guard hosts

Use this command to show the monitored host.

show nfpp icmp-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.

vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
DES-7200# show nfpp icmp-guard hosts statistics
success   fail   total
-------   ----   -----
100       20      120
```

The following example shows the monitored host:

```
DES-7200# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate
host".
VLAN  interface IP address     remain-time(s)
----   --------  ---------        -------------
1     Gi0/1     1.1.1.1     110
2     Gi0/2     1.1.2.1     61
Total: 2 host(s)
```

Related commands

Command	Description
clear nfpp icmp-guard hosts	Clear the monitored host.

12.13.2 show nfpp icmp-guard summary

Use this command to show the configurations.

show nfpp icmp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp icmp-guard summary
（Format of column Rate-limit and  Attack-threshold is p
er-src-ip/per-src-mac/per-port.）
Interface      Status      Isolate-period   Rate-limit
Attack-threshold
Global     Enable  300            4/-/60    8/-/100
Gi 0/1      Enable  180            5/-/-      8/-/-
Gi 0/2      Disable 200            4/-/60    8/-/100

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

	-	No configuration.

Related commands

Command	Description
icmp-guard attack-threshold	Set the global attack threshold.
icmp-guard enable	Enable the ICMP anti-attack function.
icmp-guard isolate-period	Set the global isolate time.
icmp-guard monitor-period	Set the monitor period.
icmp-guard monitored-host-limit	Set the maximum number of the monitored hosts.
icmp-guard rate-limit	Set the global rate-limit threshold.
nfpp icmp-guard enable	Enable the ICMP anti-attack function on the interface.
nfpp icmp-guard isolate-period	Set the isolate time.
nfpp icmp-guard policy	Set the rate-limit threshold and attack threshold.

12.13.3 show nfpp icmp-guard trusted-host

Use this command to show the trusted host free from being monitored.

show nfpp icmp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings N/A.

Command mode Privileged EXEC mode.

Usage guidelines	N/A.

Examples

```
DES-7200# show nfpp icmp-guard trusted-host
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

Related commands

Command	Description
icmp-guard trusted-host	Set the trusted host.

12.14 IP-guard Showing Related Commands

12.14.1 show nfpp ip-guard hosts

Use this command to show the monitored host.

show nfpp ip-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings	N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples	The following example shows the statistical information of the monitored host:
	`DES-7200# show nfpp ip-guard hosts statistics`
	`success fail total`
	`------- ---- -----`
	`100 20 120`
	
	`DES-7200#show nfpp ip-guard hosts`
	`If column 1 shows '*', it means "hardware do not isolate host" .`
	`VLAN interface IP address Reason remain-time(s)`
	`---- -------- --------- ------- -------------`
	`1 Gi0/1 1.1.1.1 ATTACK 110`
	`2 Gi0/2 1.1.2.1 SCAN 61`
	`Total: 2 host(s)`

Related commands

Command	Description
clear nfpp ip-guard hosts	Clear the monitored host.

12.14.2 show nfpp ip-guard summary

Use this command to show the configurations.

show nfpp ip-guard summary

Parameter description

Parameter	Description
-	-

Default Settings	N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp ip-guard summary
（Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.）
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global      Enable  300             4/-/60     8/-/100     15
Gi 0/1       Enable  180             5/-/-       8/-/-       -
Gi 0/2      Disable 200             4/-/60     8/-/100     20

Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

Related commands

Command	Description
ip-guard attack-threshold	Set the global attack threshold.
ip-guard enable	Enable the IP anti-scan function.
ip-guard isolate-period	Set the global isolate time.

ip-guard monitor-period	Set the monitor period.
ip-guard monitored-host-limit	Set the maximum number of the monitored hosts.
ip-guard rate-limit	Set the global rate-limit threshold.
nfpp ip-guard enable	Enable the IP anti-scan function on the interface.
nfpp ip-guard isolate-period	Set the isolate time.
nfpp ip-guard policy	Set the rate-limit threshold and attack threshold.

12.14.3 show nfpp ip-guard trusted-host

Use this command to show the trusted host free from being monitored.

show nfpp ip-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp ip-guard trusted-host
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

Related commands

Command	Description
ip-guard trusted-host	Set the trusted host.

12.15 ND-guard Showing Related Commands

12.15.1 show nfpp nd-guard trusted-host

Use this command to show the configurations.

show nfpp nd-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7200# show nfpp nd-guard summary
（Format of column Rate-limit and  Attack-threshold is N
S-NA/RS/RA-REDIRECT.）
Interface Status Rate-limit Attack-threshold
Global     Enable  20/5/10    40/10/20
Gi 0/1      Enable  15/15/15   30/30/30
Gi 0/2      Disable -/5/30      -/10/50
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit

	threshold for the NS-NA/RS/RA-REDIRECT.
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

Related commands

Command	Description
nd-guard attack-threshold	Set the global attack threshold.
nd-guard enable	Enable the ND anti-attack function.
nd-guard rate-limit	Set the global rate-limit threshold.
nfpp nd-guard enable	Enable the ND anti-attack function on the interface.
nfpp nd-guard policy	Set the rate-limit threshold and attack threshold.

12.16 Defined-guard Showing Related Commands

12.16.1 show nfpp define hosts

Use this command to show the monitored hosts

show nfpp define hosts *name* [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.
statistics	Show the statistics of monitored hosts.
vid	Vlan ID.
interface-id	Interface name.
ip-address	IP address.

Default Settings N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command allows filtering the hosts with parameters specified.

Examples	`DES-7200#show nfpp define hosts tcp statistics`
	`Define tcp:`
	`success fail total`
	`------- ---- -----`
	`100 20 120`
	The command execution as shown below means that there are 120 hosts monitored totally, wherein 100 hosts are isolated successfully, and 20 hosts fails.
	
	`DES-7200#show nfpp define hosts tcp`
	`Define tcp:`
	`If column 1 shows '*', it means "hardware do not isolate host" .`
	`VLAN interface IP address MAC address remain-time(s)`
	`---- -------- --------- ------------- ----------------`
	`1 Gi0/1 1.1.1.1 - 110`
	`2 Gi0/2 1.1.2.1 - 61`
	`Total: 2 host(s)`

Related commands

Command	Description
clear nfpp define hosts	Clear the monitored hosts of user-defined anti-attack type.

12.16.2 show nfpp define summary

Use this command to show the configurations

show nfpp define summary [*name*]

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command can be used to show the configurations. Without the name specified, all user-defined anti-attack types will be shown.

Examples

```
DES-7200# show nfpp define summary tcp
Define tcp summary:
match etype 0x0800 protocol 0x06
Maximum count of monitored hosts: 1000
Monitor period：300s
（Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.）
Interface Status Isolate-period Rate-limit Attack-thre
shold
Global     Enable  300            -/5/150    -/10/300
G 0/1      Enable  180           -/6/-      -/8/-
G 0/2      Disable 200            -/5/30    -/10/50
```

Field	Description
Interface	If the interface field is shown as Global, it means that is configured in the global configuration mode.
Status	Enable/ Disable the anti-attack function.

Related commands

Command	Description
match	Clear the monitored hosts of user-defined anti-attack type.

policy	Attack threshold and rate-limit threshold.
isolate-period	Isolate time
monitored-period	Monitored time
monitored-host-limit	Maximum monitored host number

12.16.3 show nfpp define trusted-host

Use this command to show the trusted host free from monitoring.

show nfpp define trusted-host *name*

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

The following example shows the trusted host configurations.

```
DES-7200# show nfpp define trusted-host tcp
Define tcp:
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

Related commands	Command	Description
	trusted-host	Configure the trusted hosts.

DES-7200

ACL&QoS Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 ACL Configuration Commands

For IDs used in the following commands, refer to the command ID table below:

ID	Meaning
ID	Number of access list. Range: Standard IP ACL: 1 to 99, 1300 to 1999 Extended IP ACL: 100 to 199,2000 to 2699 Extended MAC ACL: 700 to 799 Extended expert ACL: 2700 to 2899
name	ACL name
sn	ACL SN (products can be set according to the priority)
start-sn	Start sequence number
inc-sn	Sequence number increment
deny	If matched, access is denied.
permit	If matched, access is permitted.
port	Protocol number. For IPv6, this field can be IPv6, icmp, tcp, udp and numbers 0 to 255. For IPv4, it can be one of eigrp, gre, ipinip, igmp, nos, ospf, icmp, udp, tcp, and ip, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as icmp/tcp/udp, are listed individually.
interface *idx*	Interface index
src	Packet source IP address (host address or network address)
src-wildcard	Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.
src-ipv6-pfix	Source IPv6 network address or network type
dst-ipv6-pfix	Destination IPv6 network address or network type
pfix-len	Prefix mask length
src-ipv6-addr	Source IPv6 address
dst-ipv6-addr	Destination IPv6 address
dscp	Differential service code point, and code point value. Range:

ID	Meaning
	0 to 63
flow-label	Flow label in the range 0 to 1048575
dst	Packet destination IP address (host address or network address)
dst-wildcard	Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32
fragment	Packet fragment filtering. Note: Routers do not support the packet fragment filtering.
precedence	Packet precedence value (0 to 7)
range	The layer 4 port number range of the packet.
time-range *tm-rng-name*	Time range of packet filtering, named *tm-rng-name*
tos	Type of service (0 to 15)
cos	Class of service (0-7)
cos inner *cos*	COS of the packet tag
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name (0 to 255)
operator port[*port*]	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range) *port* indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number
src-mac-addr	Physical address of the source host
dst-mac-addr	Physical address of the destination host
VID vid	VLAN ID
VID inner vid	VID of the tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all *tcpf*	Match all bits of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface

ID	Meaning
{*rule mask offset*}$^{+}$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table "+" sign indicates at least one group

The fields in the packet are as follows:

```
AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD
DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM
NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT
UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb
```

The corresponding offset table is as follows:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol number	35
C	Data frame length field	12	Q	IP check sum	36
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP soure port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version number	26	XY	IP header length and reserved bits	58

Letter	Meaning	Offset	Letter	Meaning	Offset
K	TOS field	27	Z	Resrved bits and flags bit	59
L	Length of IP packet	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

The offsets of fields in the above table are their offsets in 802.3 data frames of SNAP+tag.

1.1 Configuration Related Commands

1.1.1 access-list

Use this command to create an access list rule to filter data packets. The **no** form of this command deletes the specified access list entries.

1. Standard IP access list (1 to 99, 1300 to 1999)

   access-list *id* {**deny** | **permit**} {*source source-wildcard* | **host** *source* | **any| interface** *idx*} [**time-range** *tm-range-name*]

2. Extended IP access list (100 to 199, 2000 to 2699)

   access-list *id* {**deny** | **permit**} **protocol** {*source source-wildcard* | **host** *source* | **any| interface** *idx* } {*destination destination-wildcard* | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

3. Extended MAC access list (700 to 799)

   access-list *id* {**deny** | **permit**} {**any** | **host** *source-mac-address*} {**any** | **host** *destination-mac-address*} [*ethernet-type*][**cos** [*out*][**inner** *in*]]

4. Extended expert access list (2700 to 2899)

   access-list *id* {**deny** | **permit**} [**protocol** | [*ethernet-type*][**cos** [*out*][**inner** *in*]]] [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**}][**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- When you select the Ethernet-type field or cos field:

  access-list *id* {**deny** | **permit**} {*ethernet-type*| **cos** [*out*][**inner** *in*]} [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host**

destination | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

  access-list *id* {deny | permit} **protocol [VID** [*out*][**inne**r *in*]] {**source**

  source-wildcard | host *source* | **any**} {**host** *source-mac-address* | **any** }

  {destination *destination-wildcard* | **host** *destination* | **any} {host**

  destination-mac-address | **any} [precedence** *precedence*] [**tos** *tos*]

  [fragment] [**range** *lower upper*] **[time-range** *time-range-name*]

  Extended expert ACLs of some important protocols:

  Internet Control Message Protocol (ICMP)

  access-list *id* {**deny** | **permit**} **icmp** [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host**

  destination-mac-address | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]]

  | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**]

  [**time-range** *time-range-name*]

  Transmission Control Protocol (TCP)

  access-list *id* {**deny** | **permit**} **tcp** [**VID** [*out*][**inner** *in*]]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [**operator** port [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

  User Datagram Protocol (UDP)

  access-list *id* {**deny** | **permit**} **udp**[**VID** [*out*][**inner** *in*]] {**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [**operator port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**}{**host** *destination-mac-address* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

5. List remark

access-list *id* **list-remark** *text*

The following parameters are described in the sequence they appear. Once described, a parameter will not be described anymore.

Parameter description

Parameter	Description
id	Access list ID. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.
deny	If not matched, access is denied.
permit	If matched, access is permitted.
source	Specify the source IP address (host address or network address).
source-wildcard	It can be discontinuous, for example, 0.255.0.32.
protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
destination	Specify the destination IP address (host address or network address).
destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
fragment	Packet fragment filtering
precedence	Specify the packet priority.
precedence	Packet precedence value (0 to 7)
range	Layer4 port number range of the packet.
lower	Lower limit of the layer4 port number.
upper	Upper limit of the layer4 port number.
time-range	Time range of packet filtering

time-range-name	Time range name of packet filtering
tos	Specify type of service.
tos	ToS value (0 to 15)
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name
operator	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)
port [*port*]	Port number; *range* needs two port numbers, while other operators only need one port number.
host *source-mac-address*	Source physical address
host *destination-mac-address*	Destination physical address
VID *vid*	Match the specified VID.
ethernet-type	Ethernet type
match-all	Match all the bits of the TCP flag.
tcp-flag	Match the TCP flag.
text	Remark information

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs:

The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses.

The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses.

The extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.

The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID.

For the layer3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence*/**tos** *tos*/**fragments**/**range** *lower upper*/**time-range** *time-range-name*

The TCP Flag includes part or all of the following:

- **urg**
- **ack**
- **psh**
- **rst**
- **syn**
- **fin**

The packet precedence is as below:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The service types are as below:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The ICMP message types are as below:

- **administratively-prohibited**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **fragment-time-exceeded**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **redirect**
- **device-advertisement**
- **device-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **ttl-exceeded**
- **unreachable**

The TCP ports are as follows. A port can be specified by port name and port number:

- **bgp**
- **chargen**
- **cmd**
- **daytime**
- **discard**
- **domain**
- **echo**
- **exec**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **ident**
- **irc**
- **klogin**
- **kshell**
- **ldp**
- **login**
- **nntp**
- **pim-auto-rp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- **biff**
- **bootpc**

- **bootps**
- **discard**
- **dnsix**
- **domain**
- **echo**
- **isakmp**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **netbios-ss**
- **ntp**
- **pim-auto-rp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

The Ethernet types are as below:

- **aarp**
- **appletalk**
- **decnet-iv**
- **diagnostic**
- **etype-6000**
- **etype-8042**
- **lat**
- **lavc-sca**
- **mop-console**
- **mop-dump**
- **mumps**
- **netbios**
- **vines-echo**
- **xns-idp**

Examples

1. Example of the standard IP ACL

The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
DES-7200 (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
DES-7200(config)#access-list 102 permit tcp any any eq domain
DES-7200(config)#access-list 102 permit udp any any eq domain
DES-7200(config)#access-list 102 permit icmp any any echo
DES-7200(config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below:

```
DES-7200(config)#access-list 702 deny host 00d0f8000c0c any aarp
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
DES-7200(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
DES-7200(config)# access-list 2702 permit any any any any
DES-7200(config)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

Related commands

Command	Description
show access-lists	Show all the ACLs.

	mac access-group	Apply the extended MAC ACL on the interface.

1.1.2 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

Use this command to set deny rules

1. Standard IP ACL

   [*sn*] **deny** {*source source-wildcard* | **host** *source* | **any| interface** *idx* }[**time-range** *tm-range-name*]

2. Extended IP ACL

   [*sn*] **deny protocol source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragment**]

   [**range** *lower upper*] [**time-range** *time-range-name*]

Extended IP ACLs of some important protocols:

- **Internet Control Message Prot** (ICMP)

  [*sn*] **deny icmp** {**source** *source-wildcard* | **host** *source* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Prot** (TCP)

  [*sn*] **deny tcp** {**source** *source-wildcard* | **host** *Source* | **any**} [*operator*

  port [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Prot** (UDP)

  [*sn*] deny udp {**source** *source –wildcard* | **host** *source* | **any**} [*operator*

  port [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

3. Extended MAC ACL

[*sn*] **deny** {**any** | **host** *source-mac-address*}{**any** | **host** *destination-mac-address*} [*ethernet-type*][**cos** [*out*] [**inner** *in*]]

4. Extended expert ACL

[*sn*] **deny**[**protocol** | [*ethernet-type][* **cos** [*out*] [**inner** *in*]*]*] [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- When you select the ethernet-type field or cos field::

sn] **deny** {[*ethernet-type}[***cos** [*out*] [**inner** *in*]*]}* [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

[*sn*] **deny protocol** [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination**

destination-wildcard | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

[*sn*] **deny icmp** [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

[*sn*] **deny tcp** [[**VID** [*out*][**inner** *in*]]]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

[*sn*] **deny udp** [[**VID** [*out*][**inner** *in*]]]{**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**}{**host**

destination-mac-address | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- **Address Resolution Protocol (ARP)**

  [*sn*] **deny arp** {**vid** *vlan-id*}[*source-mac-address source-wildcard* **|host** *source-mac-address* | **any**] [**host** *destination –mac-address* | **any**] {*sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any**} {*sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any**} {*target-ip target-ip–wildcard* | **host** *target-ip* | **any**}

5. Extended IPv6 ACL

[*sn*] **deny protocol**{*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} {*destination-ipv6-prefix / prefix-length* | **any** | *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended ipv6 ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

  [*sn*]**deny icmp** {*source-ipv6-prefix / prefix-length* | *any source-ipv6-address* | **host**} {*destination-ipv6-prefix / prefix-length* | **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** flow-label] [**fragment**] [**time-range** time-range-name]

- **Transmission Control Protocol** (TCP)

  [*sn*] **deny tcp** {*source-ipv6-prefix / prefix-length* | **host** *source-ipv6-address* | **any**}[*operator* **port**[*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

  [sn] **deny udp** {*source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**}[*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

  For the parameters that are not mentioned below, please refer to the **access-list.**

Parameter description

Parameter	Description
sn	ACL entry sequence number
source-ipv6-prefix	Source IPv6 network address or network type
destination-ipv6-prefix	Destination IPv6 network address or network type
prefix-length	Prefix mask length
source-ipv6-address	Source IPv6 address
destination-ipv6-address	Destination IPv6 address
dscp	Differential Service Code Point
dscp	Code value, within the range of 0 to 63
flow-label	Flow label
flow-label	Flow label value, within the range of 0 to 1048575.
protocol	For the IPv6, the field can be ipv6 | icmp | tcp | udp and number in the range 0 to 255
time-range	Time range of the packet filtering
time-range-name	Time range name of the packet filtering

Default configuration

N/A.

Command mode

ACL configuration mode.

Usage guidelines

N/A.

Examples

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
DES-7200(config)#expert access-list extended 2702
DES-7200(config-exp-nacl)#deny tcp  host  192.168.4.12
host 0013.0049.8272 any any
DES-7200(config-exp-nacl)#permit any any any any
DES-7200(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any
any
20 permit any any any any
DES-7200(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)# ip access-list extended ip-ext-acl
DES-7200(config-ext-nacl)# deny tcp host 192.168.4.12 eq
100 any
DES-7200(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
DES-7200(config-ext-nacl)#exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#ip access-group ip-ext-acl in
DES-7200(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#mac access-list extended mac1
DES-7200(config-mac-nacl)#deny host 0013.0049.8272 any
aarp
DES-7200(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
DES-7200(config-mac-nacl)#exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ip access-list standard 34
```

```
DES-7200(config-ext-nacl)# deny host 192.168.4.12
DES-7200(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
DES-7200(config-ext-nacl)#exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# ip access-group 34 in
```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)#11 deny ipv6 host
192.168.4.12 any
DES-7200(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
DES-7200(config-ipv6-nacl)# exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# ipv6 traffic-filter v6-acl in
```

Related commands

Command	Description
show access-list	Show all the ACLs.
ipv6 traffic-filter	Apply the extended ipv6 ACL on the interface.
ip access-group	Apply the IP ACL on the interface.
match access-group	Apply the extended MAC ACL on the interface.
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.
permit	Permit the access.

1.1.3 expert access-group

Use this command to apply the specified expert ACL on the specified interface. Use the **no** form of the command to remove the application.

expert access-group {*id*|*name*} {**in**|**out**}

no expert access-group {*id*|*name*} {**in**|**out**}

		Parameter	Description
Parameter description		*id*	ID of the expert ACL (2700 to 2899)
		name	Name of the expert ACL
		in	Filter the inputting packets of the interface
		out	Filter the outputting packets of the interface

Default configuration	No Expert ACL is applied on the interface.
Command mode	Interface configuration mode.
Usage guidelines	N/A.

Examples

The following example shows how to apply the **access-list *accept*_**00d0f8xxxxxx only to Gigabit interface 1:

```
DES-7200(config)# interface GigaEthernet 0/1
DES-7200(config-if)# expert access-group
accept_00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Show the ACL configuration.

Platform description -

1.1.4 expert access-list

Use this command to create an extended expert ACL. Use the **no** form of the command to remove the ACL.

expert access-list extended {*id* | *name*}

no expert access-list extended {*id* | *name*}

Parameter description

Parameter	Description
id	ID of the extended expert ACL (2700 to 2899)
name	Name of the extended expert ACL

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

Use **show access-lists** to display the ACL configurations**.**

Examples

Create an extended expert ACL:

```
DES-7200(config)# expert access-list extended exp-acl
DES-7200(config-exp-nacl)# show access-lists expert
access-list extended exp-acl
DES-7200(config-exp-nacl)#
```

Create an extended expert ACL:

```
DES-7200(config)# expert access-list extended 2704
DES-7200(config-exp-nacl)# show access-lists
access-list extended 2704
DES-7200(config-exp-nacl)#
```

Related commands

Command	Description
show access-lists	Show the extended expert ACLs

Platform description

-

1.1.5 ip access-group

Use this command to apply a specific ACL to an interface. The **no** form of this command cancels the application.

ip access-group {*id*|*name*} {**in**|**out**} **[unreflect | reflect]**

no ip access-group {*id*|*name*} {**in**|**out**}

Parameter description

Parameter	Description
id	ID of the IP ACL (1 to 199, 1300 to 2699)
name	Name of the IP ACL
in	Filter the incoming packets of the interface.
out	Filter the outgoing packets of the interface.
unreflect	Disable the Reflexive-ACL.
reflect	Enable the Reflexive-ACL.

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

Use the **ip access-group** command to apply the specified ACL to the interface, when the firewall is enabled.

Examples

The following example applies the ACL 120 on the fastEthernet0/0 to filter the incoming packets:

```
DES-7200(config)# interface fastEthernet 0/0
DES-7200(config-if)# ip access-group 120 in
```

Related commands

Command	Description
access-list	Define the ACL.
show access-lists	Show all the ACLs.
show ip access-list	Show the IP ACL (1 to 199, 1300 to 2699, 3000 to 3199).

ip access-list

Use this command to create a standard IP ACL or extended IP ACL. Use the **no** form of the command to remove the ACL.

ip access-list {**extended** | **standard**} {*id*|*name*}

no ip access-list {**extended** | **standard**} {*id*|*name*}

Parameter description

Parameter	Description
id	ID of the ACL 1 to 99 and 1300 to 1999 for standard ACL) or 100 to 199 and 2000 to 2699 for extended ACL
name	Name of the ACL

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

There are differences between a standard ACL and an extended ACL. The extended ACL is more precise. Refer to **deny** or **permit** in the two modes. Use **show access-lists** to display the ACL configurations**.**

Examples

Create a standard ACL:

```
DES-7200(config)# ip access-list extended 123
DES-7200(config-ext-nacl)# show access-lists
ip access-list extended 123
DES-7200(config-ext-nacl)#
```

Create an extended ACL:

```
DES-7200(config)# ip access-list standard std-acl
DES-7200(config-std-nacl)# show access-lists
ip access-list standard std-acl
DES-7200config-std-nacl)#
```

Related commands

Command	Description
show access-lists	Show the ACLs.

Platform description	N/A

1.1.6 ip access-list resequence

Use this command to reassign the sequence of the IP ACL entries and enter the corresponding configuration mode. Use the **no** form of this command to restore it to the default configuration.

ip access-list resequence {*id*|*name*} *start-sn inc-sn*

no ip access-list resequence {*id*|*name*}

Parameter description

Parameter	Description
id	ACL ID
name	ACL name
start-sn	Start sequence
inc-sn	Sequence increment

Default configuration	The start sequence is 10 and the sequence increment is 10.
Command mode	Global configuration mode
Usage guidelines	You can use the **show access-lists** command to show the configuration result.

Examples

Resequence the entries of the ACL:

```
DES-7200# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
DES-7200# config
DES-7200# (config)#ip access-list resequence 1 21 43
DES-7200# (config)# exit
DES-7200# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

Related commands	**Command**	**Description**
	show access-lists	Show the ACLs.

1.1.7 ipv6 traffic-filter

Use this command to apply the specified IPV6 ACL on the specified interface. Use the **no** form of the command to remove the application.

ipv6 traffic-filter *name* {**in**|**out**}

no ipv6 traffic-filter *name* {**in** | **out**}

Parameter description		**Parameter**	**Description**
		name	Name of Ipv6 ACL
		in	Filter the incoming packets of the interface
		out	Filter the outgoing packets of the interface

Default configuration	No ACL is applied on the interface.
Command mode	Interface configuration mode.
Usage guidelines	Apply the specified IPV6 ACL on the specified interface to control the interface traffic. You can view the configuration by command **show ipv6 traffic-filter.**

Examples	The following example shows how to apply the **access-list v6-acl** to Gigabit interface Gigabit 0/1:
	`DES-7200(config)# interface GigaEthernet 0/1`
	`DES-7200(config-if)# ipv6 traffic-filter v6-acl in`

Related commands	**Command**	**Description**
	show access-group	Show the ACL configurations.

1.1.8 ipv6 access-list

Use this command to create an extended IPV6 ACL. Use the **no** form of the command to remove the ACL.

ipv6 access-list *name*

no mac access-list *name*

Parameter description

Parameter	Description
name	ACL name

Command mode

Global configuration mode.

Usage guidelines

Use **show access-lists** to view ACL configuration.

Examples

Create an extended ipv6 ACL**:**

```
DES-7200(config)# ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list v6-acl
DES-7200(config-ipv6-nacl)#
```

Related commands

Command	Description
show access-lists	Show the extended ipv6 ACLs

1.1.9 mac access-group

Use this command to apply the specified MAC ACL on the specified interface. Use the **no** form of the command to remove the application.

mac access-group {*id*|*name*}{**in**|**out**}

no mac access-group {*id*|*name*}{**in**|**out**}

Parameter description

Parameter	Description
id	ID of the MAC ACL (700 to 799)
name	Name of the MAC ACL

in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

You can use the **show running-config** command to show the configuration result.

Examples

The following example shows how to apply the **access-list accept**_00d0f8xxxxxx only to Gigabit interface 1:

```
DES-7200(config)#interface GigaEthernet 1/1
DES-7200(config-if)#mac access-group accept__00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Show the ACL configuration.

Platform description

-

1.1.10 mac access-list

Use this command to create an extended MAC ACL. Use the **no** form of the command to remove the ACL.

mac access-list extended { *id*|name }

no mac access-list extended {*id*|*name*}

Parameter description

Parameter	Description
id	ID of the extended MAC ACL (700 to 799)
name	Name of the extended MAC ACL

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	Use **show access-lists** to display the ACL configurations**.**

Examples	Create an extended MAC ACL**:**
	`DES-7200(config)# mac access-list extended mac-acl`
	`DES-7200(config-mac-nacl)# show access-lists mac access-list extended mac-acl`
	Create an extended ACL:
	`DES-7200(config)# mac access-list extended 704`
	`DES-7200(config-mac-nacl)# show access-lists mac access-list extended 704`

Related commands

Command	Description
show access-lists	Show the extended MAC ACLs

Platform description	-

1.1.11 no sn

Use this command to delete an entry of the ACL.

no <*sn*>

Parameter description

Parameter	Description
sn	Sequence number of the ACL entry

Command mode	ACL configuration mode.
Usage guidelines	Use this command to delete an ACL entry in ACL configuration mode.

Examples

```
DES-7200(config)# ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)# permit ipv6
host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)#12 deny ipv6 host any any
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
12 deny ipv6 any any
DES-7200(config-ipv6-nacl)# no 12
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)#
```

Related commands

Command	Description
show access-list	Show all the ACLs.
ip access-list	Define the IP ACL.
ipv6 access-list	Define the extended IPV6 ACL.
deny	Define the deny rule.
permit	Define the permit rule.

1.1.12 permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

Use this command to set the permit rules.

1. Standard IP ACL

[*sn*] **permit** {*source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*]

2. Extended IP ACL

[*sn*] **permit protocol source** *source-wildcard* **destination**

destination-wildcard [**precedence** *precedence*] [**tos** *tos*] **[fragment]**

[**time-range** *time-range-name*]

Extended IP ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

[*sn*] **permit icmp** {**source** *source-wildcard* | **host** *source* | **any**}

{**destination** *destination-wildcard* | **host** *destination* | **any**}

[*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

  [*sn*] **permit tcp** {**source** *source-wildcard* | **host** *Source* | **any**} [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

  [*sn*] **permit udp** {**source** *source -wildcard*|**host** *source* |**any**} [*operator* **port** [*port*]] {**destination** *destination-wildcard* |**host** *destination* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

3. Extended MAC ACL

[*sn*] **permit** {**any** | **host** *source-mac-address*} {**any** | **host**

destination-mac-address} [*ethernet-type*][**cos** [*out*] [**inner** *in*]]

4. Extended expert ACL

[*sn*] **permit** [**protocol** | [*ethernet-type][* **cos** [*out*] [**inner** *in*]*]*] [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source*-mac-*address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**time-range** *time-range-name*]

- When you select the Ethernet-type field or cos field:

  [*sn*] **permit** {*ethernet-type*| **cos** [*out*] [**inner** *in*]*}* [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

  [*sn*] **permit protocol** [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

  [*sn*] **permit icmp** [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**}[*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

  [*sn*] **permit tcp** [**VID** [*out][***inner** *in]*]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

  [*sn*] **permit udp** [**VID** [*out][***inner** *in]*]{**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

5. Extended IPv6 ACL

[*sn*] **permit protocol** {*source-ipv6-prefix / prefix-length* | **any** | **host** *source-ipv6-address*} {*destination-ipv6-prefix / prefix-length* | **any** | *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

Extended IPv6 ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

  [*sn*] **permit icmp** {*source-ipv6-prefix / prefix-length* | **any**

  source-ipv6-address | **host**} {*destination-ipv6-prefix / prefix-length*

  | **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type*

  [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*]

  [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

  [*sn*] **permit tcp** {*source-ipv6-prefix / prefix-length* | **host**

source-ipv6-address | **any**} [*operator* **port** [*port*]]

{*destination-ipv6-prefix / prefix-length* | **host**

destination-ipv6-address | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*]

[**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

[**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

[*sn*] **permit udp** {*source-ipv6-prefix / prefix-length* | **host**

source-ipv6-address | **any**} [*operator* **port** [*port*]]

{*destination-ipv6-prefix / prefix-length* | **host**

destination-ipv6-address | **any**} [*operator* **port** [**port**]] [**dscp** *dscp*]

[**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

Parameter description	For those not listed below, see **deny**.
Default configuration	N/A.
Command mode	ACL configuration mode.
Usage guidelines	Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.
Examples	The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
DES-7200(config)#expert access-list extended exp-acl
DES-7200(config-exp-nacl)#permit tcp  host
192.168.4.12 host 0013.0049.8272 any any
DES-7200(config-exp-nacl)#deny any any any any
DES-7200(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any
any
20 deny any any any any
DES-7200(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)# ip access-list extended 102
DES-7200(config-ext-nacl)# permit tcp host 192.168.4.12
eq 100 any
DES-7200(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
DES-7200(config-ext-nacl)#exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#ip access-group 102 in
DES-7200(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#mac access-list extended 702
DES-7200(config-mac-nacl)#permit host 0013.0049.8272 any
aarp
DES-7200(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
DES-7200(config-mac-nacl)#exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ip access-list standard std-acl
DES-7200(config-std-nacl)#permit host 192.168.4.12
DES-7200(config-std-nacl)#show access-lists
ip access-list standard std-acl
  10 permit host 192.168.4.12
DES-7200(config-std-nacl)#exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL.

The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)#11 permit ipv6
host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)# exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#ipv6 traffic-filter v6-acl in
```

Related commands

Command	Description
show access-lists	Show all the ACLs.
ipv6 traffic-filter	Apply the extended ipv6 ACL on the interface.
ip access-group	Apply the IP ACL on the interface.
match access-group	Apply the extended MAC ACL on the interface.
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.
deny	Deny the access.

1.2 Showing Related Commands

1.2.1 show access-group

Use this command to show the ACL configured on the interface.

show access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode
Usage guidelines	Show the ACL configured of the interface. If no interface is specified, the associated ACLs of all the interfaces will be shown.

Examples	`DES-7200# show access-group`
	`ip access-list standard ipstd3`
	`Applied On interface GigabitEthernet 0/1.`
	`ip access-list standard ipstd4`
	`Applied On interface GigabitEthernet 0/2.`
	`ip access-list extended 101`
	`Applied On interface GigabitEthernet 0/3.`
	`ip access-list extended 102`
	`Applied On interface GigabitEthernet 0/8.`

Related commands

Command	Description
ip access-group	Apply the IP ACL to the interface.
mac access-group	Apply the mac ACl to the interface.
expert access-group	Apply the expert ACL to the interface.
ipv6 traffic-filter	Apply the IPv6 ACL to the interface.

1.2.2 show access-lists

Use this command to show all ACLs or the specified ACL.

show access-lists [*id*|*name*]

Parameter description

Parameter	Description
id	ID of the IP ACL
name	Name of the IP ACL

Command mode	Privileged mode.

Usage guidelines

Use this command to show the specified ACL. If no ID or name is specified, all the ACLs will be shown.

Examples

```
DES-7200# show access-lists n_acl
ip access-list standard n_acl
DES-7200# show access-lists 102
ip access-list extended 102
DES-7200# show access-lists
ip access-list standard n_acl
ip access-list extended 101
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
```

Related commands

Command	Description
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.

1.2.3 show expert access-group

Use this command to show the configured expert ACL of the interface.

show expert access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode

Privileged mode.

Usage guidelines

Show the expert ACL configured on the interface. If no interface is specified, the associated expert ACLs of all the interfaces will be shown.

Examples

```
DES-7200# show expert access-group interface
gigabitethernet 0/2
expert access-group ee in
```

```
Applied On interface GigabitEthernet 0/2.
```

Related commands

Command	Description
expert access-list	Define the extended expert ACL.

1.2.4 show ip access-group

Use this command to show the IP ACL configured on the interface.

show ip access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode

Privileged mode

Usage guidelines

Show the IP ACL configured of the interface. If no interface is specified, the associated IP ACLs of all the interfaces will be shown.

Examples

```
DES-7200# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

Related commands

Command	Description
ip access-list	Define the IP ACL.

1.2.5 show ipv6 traffic-filter

Use this command to show the configured IPv6 ACL of the interface.

show ipv6 traffic-filter[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode.
Usage guidelines	Show the IPv6 ACL associated with the interface. If no interface is specified, the associated IPv6 ACLs of all the interfaces will be shown.
Examples	DES-7200# **show ipv6 traffic-filter interface gigabitethernet** *0/4* ipv6 access-group v6 in Applied On interface GigabitEthernet 0/4.

Related commands

Command	Description
ipv6 access-list	Define the type of IPv6 ACL.

1.2.6 show mac access-group

Use this command to show the configured MAC ACL of the interface.

show mac access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode.
Usage guidelines	Show the MAC ACL associated with the interface. If no interface is specified, the associated MAC ACLs of all associated interfaces will be shown.
Examples	DES-7200# **show mac access-group interface gigabitethernet** *0/3* mac access-group *mm* in Applied On interface GigabitEthernet 0/3.

Related

Command	Description

commands	**mac access-list**	Define the extended MAC ACL.

1.3 Security Channel

1.3.1 security global access-group

Use this command to configure the global security channel.

security global access-group { *id* | *name* **}**

no security global access-group

Parameter description

Parameter	Description
id	ACL ID
name	ACL name

Command mode Global configuration mode

Usage guidelines Use this command to configure the global security channel .

Examples

```
DES-7200# security global access-group 1
```

Platform description -

1.3.2 security access-group

Use this command to configure the security channel on the interface.

security access-group { *id* | *name* **}**

no security access-group

Parameter description

Parameter	Description
id	ACL ID

	name	ACL name

Command mode	Interface configuration mode.
Usage guidelines	Use this command to configure the security channel on the interface.
Examples	`DES-7200# security access-group 1`
Platform description	-

1.3.3 security uplink enable

Use this command to configure the uplink port of the security channel on the interface.

security uplink enable

no security uplink enable

Command mode	Interface configuration mode.
Usage guidelines	Use this command to configure the uplink port of the security channel on the interface.
Examples	`DES-7200# security uplink enable`
Platform description	-

1.3.4 show security

Use this command to show security channel configuration or the configuration of the security channel on the specified interface.

show secu-acl

Parameter	**Parameter**	**Description**

description	-	-

Default configuration N/A

Command mode Privileged mode

Usage guidelines This command is used to show all security channels.

Examples

```
DES-7200(config-if)#show secu-acl
Ports     Type      access-group
---------- ---------- ------------
Fa0/4     security   50
Global    security   60
Fa0/6     uplink     --
```

Related commands

Command	Description
security global access-group	Define the global security channel.
security access-group	Define the security channel on the interface.
security uplink enable	Define the uplink port of the security channel on the interface.

Platform description -

1.4 SVI Router ACLs Configuration Commands

1.4.1 svi router-acls enable

Use this command to enable the svi router-acls function to validate the SVI ACL on the routing packets only forwarded by Layer-3 devices. Use the **no** form of this command to disable this function

svi router-acls enable

[*no*] **svi router-acls enable**

Parameter description

Parameter	Description
no	Disable the svi router-acls function.

Default configuration Disabled.

Command mode Global configuration mode

Usage guidelines N/A

Examples

```
DES-7200#svi router-acls enable
```

Related commands

Command	Description
-	-

Platform description This command is supported by the DES-7200 series switches

2 QoS Configuration Command

2.1 Default Configuration

Before configuring QoS, you must have a full knowledge of these items related to QoS:

1. One interface can only be associated with one policy map at most.
2. One policy map may own many class maps
3. One class map can be associated with only one ACL, and all the ACEs of this ACL must have the same filter domain template.
4. The number of ACEs associated with an interface complies with the restriction given in "*Configuring Security ACLs*".

The QoS function is disabled by default. Namly the device processes all the packets in the same way. But if you associate a policy map with an interface and the trust mode on one interface, the QoS of this interface is enabled automatically. To disable the QoS function of the interface, simply resolve the policy map setting of the interface and set the information mode of the interface to Off. Below is the default QoS configuration:

Default CoS value	0
Queue Number	8
Queue Scheduling	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:15
DRR Weight Range	1:15
Trust mode	No Trust

Default CoS to queue mapping table:

CoS Value	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Default CoS to DSCP mapping table

CoS Value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

Default IP Precedence to DSCP mapping table

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default DSCP to CoS mapping table

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

2.2 Related Configuration Commands

2.2.1 mls qos trust

Use this command to configure the trust mode on an interface. Use the no form of this command to restore it to the default.

mls qos trust [cos | dscp | ip-precedence]

no mls qos trust

Parameter description

Parameter	Description
cos	The QoS trust mode of the port is CoS.
dscp	The QoS trust mode of the port is DSCP.
ip-precedence	The QoS trust mode of the port is IP-PRE.
no	Restore it to the default value.

Default configuration N/A.

Command mode	Interface configuration mode.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# mls qos trust cos`
Related commands	**show mls qos interface** *interface-id*
Platform description	DES-7200 series support the parameter **cos dscp ip-precedence.**

2.2.2 mls qos cos

Use this command to configure the CoS value of an interface. Use the no form of this command to restore it to the default.

mls qos cos *default-cos*

no mls qos cos

Parameter description

Parameter	Description
default-cos	0~7
no	Restore it to the default value.

Default configuration	The CoS value is 0.
Command mode	Interface configuration mode.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# mls qos cos 7`
Related commands	**show mls qos interface** *interface-id*

2.2.3 interface rate-limit

Use this command to set the rate limit on the port.

rate-limit { **input | output** } *bps burst-size*

no rate-limit

Parameter description

Parameter	Description
input	Input rate limit
ouput	Ouput rate limit
bps	Limited bandwidth per second
burst-size	The dscp-list range varies with products
no	Restore it to the default value.

Default configuration N/A

Command mode Interface configuration mode.

Examples

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# rate-limit input 1000000 4096
```

Related commands

Command	Description
show mls qos interface	-

2.2.4 class maps

Use the following command to creat an ACL:

ip access-list {**extended | standard**} { *acl-id* | a*cl-name* }

Or **mac access-list extended** {*acl-id* | a*cl-name*}

Or **expert access-list extended** {*acl-id* | a*cl-name*}

Or **ipv6 access-list extended** a*cl-name*

Or **access-list** *acl-id* series commands (refer to the related ACL chapters)

Use the following command to create a class map and enter the class map configuration mode:

[no] class-map *class-map-name*

Use the following command to create the matching standard of class map:

[**no**] **match access-group** a*cl-name*| *acl-id*

[**no**] **match ip dscp** dscp-value1 [dscp-value2 [dscp-valueN]]

[**no**] **match ip precedence** *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]

Parameter description

Parameter	Description
acl-name	Name of the created ACL
acl-id	ID of the created ACL
class-map-name	Name of the class map to be created
dscp-valueN	Ip dscp value to be created.
ip-pre-valueN	Ip precedence value to be created.
no class-map *class-map-name*	Delete the existed class map.
no match access-group a*cl-name*| *acl-id*	Delete the match.
no match ip dscp *dscp-value1* [*dscp-value2* [*dscp-valueN*]]	Delete the matched ip dscp value.
no match ip precedence *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]	Delete the matched ip precedence value.

Command mode

Global configuration mode.

Examples

Create an extended MAC ACL named me.

```
DES-7200(config)# mac access-list extended me
```

Set ACL rules.

```
DES-7200(config-ext-macl)# permit host 1111.2222.3333 any
```

Exit the ACL setting.

```
DES-7200(config-ext-macl)# exit
```

Create a class map named **cm.**

```
DES-7200(config)# class-map cm
```

Associate the class map and the ACL.

```
DES-7200(config-cmap)# match access-group me
```

Exit the class map setting.

	DES-7200(config-cmap)# **exit** Create the class-map naming cm-dscp and match the DSCP 8,16,24 and exit the setting DES-7200(config)# **class-map cm-dscp** DES-7200(config-cmap)# **match ip dscp** *8 16 24* DES-7200(config-cmap)# **exit**

Related commands	**Command**	**Description**
	show map access-lists	-
	show ip access-lists	-
	show class-map	-

Platform description	The none-tos function is supported on the DES-7200 series device.

2.2.5 policy maps

Use the following command to create a policy map and enter the policy map configuration mode

[no] policy-map *policy-map-name*

Use the following command to create the class map data classification used in the policy map and enter into the data classification configuration mode.

[no] class *class-map-name*

Use the following command to set the ip_dscp value of the IP packets, which does not take effect for non-IP packets.

set ip dscp *new-dscp*

no set ip dscp

Use the following command to set the cos value of the packets. With the **none-tos** configured, the DSCP value of the packets will not be modified.

set cos *new-cos* [none-tos]

no set cos

Use the following command to limit the bandwidth and specify the method of handling the excessive part.

police *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**] }]

no police

Parameter description

Parameter	Description
policy-map-name	Name of the policy map to be created
no policy-map *policy-map-name*	Delete the existed policy map.
class-map-name	Name of the created class map
no class *class-map-name*	Delete the class map.
new-dscp	New DSCP value, whose range varies with products.
new-cos	New Cos value, in the range of 0 to 7.
rate-bps	The limitation of bandwidth per second, in kbps
burst-byte	The burst traffic limitation, in Kbyte
drop	Drop the packets exceeding the bandwidth.
dscp-value	Overwrite the DSCP value of the packets exceeding the bandwidth, whose range varies with products.
cos-value	Modify the Cos value of the packet of over-bandwidth, in the range of 0 to 7.

Command mode

Global configuration mode

Examples

Create a policy map and name it as **po**

```
DES-7200(config)# policy-map po
```

Associate class-map cm

```
DES-7200(config-pmap)# class cm
```

Set the DSCP value as 10

```
DES-7200(config-pmap-c)# set ip dscp 10
```

Set the bandwidth as 1M, the burst traffic as 4096k, and the method for handing the excessive part to assign the new DSCP value of 16**.**

```
DES-7200(config-pmap-c)# police 1000000 4096
exceed-action dscp 16
```

Related commands	**show policy-map**
Platform description	This command is supported on the DES-7200 series devices. The DES-7200 series support the Cos modifying.

2.2.6 service-policy

Use this command to apply the policy map on the interface or the virtual-group.

service-policy {**input | output**} *policy-map-name*

no service-policy {**input | output**}

Parameter description

Parameter	Description
policy-map-name	Name of the created policy map
no	Cancel the application of the policy map on the interface or the virtual-group.

Command mode	Interface configuration mode, and virtual-group configuration mode.

Examples

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# service-policy input po
DES-7200(config)# virtual-group 3
DES-7200(config-if)# service-policy input po
```

Related commands	**show mls qos interface.**
Platform description	DES-7200 series support the parameter **input** and **output.** The parameter **output** is not supported in the virtual-group.

2.2.7 priority-queue

Use this command to configure the output queue scheduling algorithm.

priority-queue

[no] priority-queue

Parameter description

Parameter	Description
priority-queue	Set the output queue scheduling algorithm to SP (for DES-7200).
no priority-queue	Set the output queue scheduling algorithm to WRR.

Default configuration The output queue scheduling algorithm is WRR.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# no priority-queue
```

Related commands **show mls qos queuing**

53.2.8 priority-queue cos-map

Use this command to configure the associated CoS value of output queue:

priority-queue cos-map *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]

no priority-queue cos-map

Parameter description

Parameter	Description
qid	Specified queue id.
cos0 ... cos7	Associated CoS value.
no	Restore to the default value.

Default configuration See default configuration.

Command mode Global configuration mode.

Examples	`DES-7200(config)#priority-queue cos-map 1 0 1`
Related commands	**show mls qos queuing**

2.2.8 wrr-queue bandwidth

Use this command to set the weight ratio for the WRR algorithm. Use the **no** form of the command to restore it to the default.

wrr-queue bandwidth *weight1 ... weightn*

no war-queue bandwidth

Parameter description

Parameter	Description
weight1...weightn	Weight value specified for the output queues. For the number of weights and its range, see the default settings.
no	Restore to the default value.

Default configuration	weight1: ...: weightn = 1:..:1
Command mode	Global configuration mode
Examples	`DES-7200(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8`
Related commands	**show mls qos queuing**

2.2.9 mls qos map cos-dscp

Use this command to map the CoS value to the DSCP value. Use the **no** form of the command to disable the mapping.

mls qos map cos-dscp *dscp1...dscp8*

no mls qos map cos-dscp

Parameter description

Parameter	Description
dscp	Specify the DSCP value.
no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode

Examples

```
DES-7200(config)# mls qo map cos-dscp 8 10 16 18 24 26 32 34
```

Related commands

Command	Description
show mls qos maps	Show DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

2.2.10 mls qos map dscp-cos

Use this command to map the DSCP value to the COS value. Use the **no** form of the command to disable the mapping.

mls qos map dscp-cos *dscp-list* to *cos*

no mls qos map dscp-cos

Parameter description

Parameter	Description
dscp-list	DSCP list. Its range varies with products.
cos	COS value ranging 0 to 7
no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

Related commands	Command	Description
	show mls qos maps	Show DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

2.2.11 interface rate-limit

Use this command to configure rate limitation on the interface. Use the **no** form of the command to restore it to the default.

rate-limit {**input** | **output**} *bps burst-size*

no rate-limit

Parameter description	Parameter	Description
	input	Specify the input speed limit.
	output	Specify the output speed limit.
	bps	Bandwidth limitation per second
	burst-size	Burst traffic limit (Kbyte). Its range varies with products.
	no	Restore to the default value.

Command mode Interface configuration mode.

Examples

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# rate-limit input 1000000 4096
```

Related commands **show mls qos interface.**

2.2.12 mls qos scheduler

Use this command to configure the queue scheduling algorithm. Use the **no** form of the command to restore it to the default.

mls qos scheduler [**sp | rr | wrr | drr**]

no mls qos scheduler

Parameter description	Parameter	Description
	sp	Absolute priority scheduling
	rr	Round-robin scheduling

	wrr	Frame count weighted round-robin scheduling
	drr	Frame length weighted round-robin scheduling
	no	Restore to the default value.

Default configuration The queue scheduling algorithm is wrr by default.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# mls qos scheduler sp
```

Related commands **show mls qos scheduler.**

2.2.13 drr-queue bandwidth

Use this command to set the queue weight in the DRR scheduling mode. Use the **no** form of the command to restore it to the default.

drr-queue bandwidth *weight1...weight8*

no drr-queue bandwidth

Parameter description	**Parameter**	**Description**
	weight1...weight8	Queue weight. For the value range, see the default configuration.
	no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# drr-queue bandwidth 1 2 3 4 5 6 7 8
```

Related commands	**show mls qos queuing**

2.2.14 mls qos map ip-prec-dscp

Use this command to map the IP-precedence to the DSCP value. Use the **no** form of this command to disable the mapping.

mls qos map ip-prec-dscp dscp1...dscp8

no mls qos map ip-prec-dscp

Parameter description

Parameter	Description
dscp	Specify the DSCP value.
no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34
```

Related commands

Command	Description
show mls qos maps	Show the DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

2.2.15 virtual-group

Use this command to configure a physical port or Aggregate port as the member port of a virtual group. Use the **no** form of this command to remove the member attribute of a virtual group on the port.

virtual-group *virtual-group-number*

no virtual-group *virtual-group-number*

Parameter description

Parameter	Description
virtual-group-number	Virtual group number, up to 128.

Default configuration	By default, the physical port belongs to no virtual-group.
Command mode	Interface configuration mode.
Usage guidelines	The member port joined the virtual group must be physical port or Aggregate Port. The virtual group member ports must be in the same line card(for the chassis-shaped switch) or in the same switch(for the box-shaped switch). If the line card or switch has 48 ports, then all member ports shall be distributed on the former 24 ports or the latter 24 ports.

Examples	The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3:
	`DES-7200(config)# interface gigabitethernet 1/3`
	`DES-7200(config-if)# virtual-group 3`

Related commands

Command	Description
show virtual-group	Show the virtual-group settings.

2.3 Showing Related Command

2.3.1 show class-map

Use this command to show the information of class maps.

show class-map [*class -name*]

Parameter description

Parameter	Description
class-name	Name of the class map

Default configuration	All class maps are shown by default.

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show class-map`

2.3.2 show policy-map

Use this command to show the information of the policy map.

show policy-map [*policy-name* [**class** *class-name*]]

Parameter description

Parameter	Description
policy-name	Name of the policy name
class-name	Name of the class map

Default configuration	All policy maps are shown by default.
Command mode	Privileged EXEC mode.
Examples	`DES-7200# show policy-map`

2.3.3 show mls qos interface

Use this command to display the QoS configuration on the interface.

show mls qos interface [*interface-id*] [**policers**]

Parameter description

Parameter	Description
interface-id	Interface ID
policers	Show the police associated with the interface

Default configuration	The QoS information of all ports is shown.

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show mls qos interface fastEthernet 0/1`

2.3.4 show mls qos queuing

Use this command to show the QoS queuing information.

show mls qos queueing

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show mls qos queueing`
Platform description	DES-7200 series show cos-to-queue map, wrr weight, and drr weight.

2.3.5 show mls qos scheduler

Use this command to show the information on queue scheduling algorithm.

show mls qos scheduler

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show mls qos scheduler`
Platform description	This command is supported on DES-7200 series.

2.3.6 show mls qos maps

Use this command to show QoS maps.

show mls qos maps [**cos-dscp | dscp-cos | ip-prec-dscp**]

Parameter description

Parameter	Description
cos-dscp	Show the cos-dscp maps.
dscp-cos	Show the dscp-cos maps.

	ip-prec-dscp	Show the ip-prec-dscp maps.

Default configuration All QoS maps are shown by default.

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show mls qos maps
```

2.3.7 show mls qos rate-limit

Use this command to show the information about rate limit on the interface.

show mls qos rate-limit [**interface** *interface-id*]

Parameter description

Parameter	Description
interface	Interface ID

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show mls qos rate-limit
```

2.3.8 show virtual-group

Use this command to show the virtual group information.

show virtual-group [*virtual-group-number* | **summary**]

Parameter description

Parameter	Description
virtual-group-number	Virtual group number, up to 128.
summary	Show the information on all virtual groups.

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show virtual-group 1

DES-7200# show virtual-group summary
```

Related commands

Command	Description
virtual-group	Enable the virtual group.

3 MPLS QOS Configuration Commands

3.1 Default Configurations

MPLS QoS allows the differentiation of MPLS packets. Since MPLS QoS is a subset of QoS, the previous section (QoS Configuration commands) is called IP QoS to facilitate description.

Before proceeding with MPLS QoS configuration, the following information related to MPLS QoS shall be clarified:

- All configurations of IP QoS are applicable to MPLS QoS;
- MPLS QoS allows the differentiation of MPLS packets;
- When one or multiple label is inserted into an IP packet, the default action is the map internal CoS to all EXP bits added into the label as per cos-exp mapping relation.
- Support one group of exp-cos maps and 8 groups of cos-exp maps.

By default, MPLS QoS function is disabled, namely the device will treat all packets equally. The following tables show the default configurations of MPLS QoS:

Default EXP-to-CoS map

	EXP value	CoS value
EXP to CoS	0	0
	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7

Default CoS-EXP map

CoS to EXP

CoS	EXP
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Usage guidelines

Caution The contents in 8 groups of default cos-exp maps are the same.

Note Currently, MPLS QoS is supported by DES-7200 series products based on EC line card.

3.2 Configuration Related Commands

3.2.1 match mpls experimental topmost

Match one or multiple EXPs. Use this command in class-map configuration mode. Use **no** form of this command to remove matched EXP values from one class map.

match mpls experimental topmost *exp-value1* [*exp-value2* [*exp-valueN*]]

no match mpls experimental topmost *exp-value1* [*exp-value2* [*exp-valueN*]]

Parameter description

Parameter	Description
exp-valueN	EXP value to be matched; up to 8 different values can be matched at one time.

Default No matching rule.

Command mode	Class-map configuration mode.
Usage guidelines	The range of EXP value is 0-7.

Examples	The following example shows how to match multiple EXP values. 3 EXP values are matched in this example.
	`DES-7200(config)# class-map map1`
	`DES-7200(config-cmap)# match mpls experimental topmost 1 2 3`
	`DES-7200(config-cmap)# exit`

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.
match ip dscp	Match the DSCP value of packet (only applies to IPv4 packets).
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
service-policy	Associate one policy map to the specified interface.
set cos	Mark the CoS value of packet
show class-map	Display the specific contents of all class maps or the specified class map.

Platform description	This command is supported by DES-7200 series devices based on EC line card.

3.2.2 mls qos map exp-cos

Use this command to set mapping the EXP value to the packet CoS value. Use **no** form of this command to the restore to the default exp-cos mapping relation.

mls qos map exp-cos *cos1 cos2 cos3 cos4 cos5 cos6 cos7 cos8*

no mls qos map exp-cos

Parameter description

Parameter	Description
cos1...cos8	Define EXP-to-CoS mapping. These 8 values (cos1-cos8) correspond to EXP values of 0-7.

Default	See the default EXP-CoS map given in the section of "Default Configurations".
Command mode	Global configuration mode.
Usage guidelines	NA.

Examples

```
DES-7200# configure terminal
DES-7200(config)# mls qos exp-cos 1 1 2 2 5 6 7 8
```

Related commands

Command	Description
show mls qos maps	Display configurations of QoS mapping relation.

Platform description	This command is supported by DES-7200 series devices based on EC line card.

3.2.3 mls qos map cos-exp

Use this command to set mapping the CoS value to the EXP value. Use **no** form of this command to the restore to the default cos-exp mapping relation.

mls qos map cos-exp *group-number exp1 exp2 exp3 exp4 exp5 exp6 exp7 exp8*

no mls qos map cos-exp *group-number*

Parameter description

Parameter	Description
group-number	Number of cos-exp mapping group (1-8).
exp1...exp8	Define CoS-to-EXP mapping. These 8 values (exp1-exp8) correspond to CoS values of 0-7.

Default	See the default CoS-EXP map given in the section of "Default Configurations".
Command mode	Global configuration mode.
Usage guidelines	If the user doesn't to map which cos-exp mapping group to a specific interface, then all cos-exp mapping groups applied to this interface will be the first group by default.

Examples	Example: Configure the first group of cos-exp map.
	`DES-7200# configure terminal`
	`DES-7200(config)# mls qos map cos-exp 1 0 2 1 3 3 5 6 7`

Related commands

Command	Description
show mls qos maps	Display configurations of QoS mapping relation.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.2.4 mls qos service cos-exp

Associate a cos-exp mapping group to the interface. Use **no** form of this command to restore to the first group.

mls qos service cos-exp *group-number*

no mls qos service cos-exp

Parameter description

Parameter	Description
group-number	Number of cos-exp mapping group (1-8).

Default

By default, the first group of cos-exp map is associated to the interface.

Command mode

Interface configuration mode.

Usage guidelines

Caution

Cos-exp mapping relation only applies to egress packets.

Note

By default, the contents in 8 groups of default cos-exp maps are the same.

Usage guidelines

NA

Examples

Example: Associate the third group of cos-exp map to interface Gi 1/1.

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mls qos service cos-exp 3
```

Related commands

Command	Description
mls qos map cos-exp	Map CoS value to the EXP value.
show mls qos interface *interface-id*	Display QoS information related to the interface.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.2.5 mls qos trust

Configure QoS trust mode on the interface. Use **no** form of this command to restore the interface to the default trust mode.

mls qos trust {cos | dscp | ip-precedence | experimental}

no mls qos trust

Parameter description

Parameter	Description
cos	QoS trust mode of the interface is trust CoS.
dscp	QoS trust mode of the interface is trust DSCP.
ip-precedence	QoS trust mode of the interface is trust IP-PRE.
experimental	QoS trust mode of the interface is trust MPLS EXP.

Default

Untrusted.

Command mode	Interface configuration mode.
Usage guidelines	NA.

Examples	Example: Configure the trust mode of port Gi 1/1 to trust MPLS EXP.
	`DES-7200(config)# interface gigabitethernet 1/1`
	`DES-7200(config-if)# mls qos trust experimental`

Related commands

Command	Description
show mls qos interface *interface-id*	Display QoS information related to the interface.

Platform description	The QoS trust mode as trust MPLS EXP is supported by DES-7200 series products based on EC line card.

3.2.6 mpls copy experimental

Enable the MPLS EXP copying. The EXP bits in the incoming topmost label will be copied to the outgoing label to be exchanged. When the ingress label is removed, the EXP bits in the original incoming topmost label will be copied to the second topmost label. Use **no** form of this command to disable MPLS EXP copying.

[no] mpls copy experimental

Parameter description

Parameter	Description
-	-

Default	MPLS EXP copying is disabled.
Command mode	Global configuration mode.

Usage guidelines	NA

Examples	Example: Enable the MPLS EXP copying.
	`DES-7200# configure terminal`
	`DES-7200(config)# mpls copy experimental`

Related commands

Command	Description
show mls qos mpls	Display MPLS QoS information.

Platform description	This command is supported by DES-7200 series devices based on EC line card.

3.2.7 mpls propagate-experimental none

When configuring to remove the label, the EXP bits in the original incoming topmost label won't be copied to the second topmost label. Use **no** form of this command to restore the copying of EXP bits in the incoming topmost label to the second topmost label.

[no] mpls propagate-experimental none

Parameter description

Parameter	Description
-	-

Default	This function is disabled.
Command mode	Global configuration mode.
Usage guidelines	Before configuring "**mpls propagate-experimental none**", you must configure "**mpls copy experimental**" command first.

Examples

Example: When configuring to remove the label, the EXP bits in the original incoming topmost label won't be copied to the second topmost label.

```
DES-7200# configure terminal
DES-7200(config)# mpls copy experimental
DES-7200(config)# mpls propagate-experimental none
```

Related commands

Command	Description
mpls copy experimental	Enable the MPLS EXP copying.
show mls qos mpls	Display the MPLS QoS information.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.2.8 police

Limit the bandwidth for the specified traffic and specify the action for handling excessive traffic. Use **no** form of this command to disable traffic limit.

police *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**]}]

no police

Parameter description

Parameter	Description
rate-bps	Limit the bandwidth per second (unit: kbps).
burst-byte	Limit the burst traffic (unit: kbyte).
drop	Discard excessive packets.
dscp-value	Change the DSCP value of excessive packets.
cos-value	Change the CoS value of excessive packets (range: 0-7).

	none-tos	The DSCP value of excessive packets won't be modified while changing the CoS value of excessive packets.

Default

Drop excessive packets.

Command mode

Data classification configuration mode.

Usage guidelines

This command is used to mark the CoS value of packets. Use this command to modify the CoS value of packets, and the use the cos-exp map attached to the interface to indirectly modify the MPLS EXP value of egress packets.

Examples

Example: Match MPLS packets with MPLS EXP being 2 and classify these packets into the class of exp-2. Configure policy to rate limit the incoming packets and mark the CoS value of excessive packets as 0 (assuming that the input interface of MPLS packets is gigabitethernet 2/2).

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# class-map exp-2
DES-7200(config-cmap)# match mpls experimental topmost 2
DES-7200(config-cmap)# exit
DES-7200(config)# policy-map policy-for-exp2
DES-7200(config-pmap)# class exp-2
DES-7200(config-pmap-c)# police 1000000 4096 exceed-action cos 0
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
DES-7200(config)# interface gigabitethernet 2/2
DES-7200(config-if)# service-policy input
```

```
policy-for-exp2
DES-7200(config-if)# exit
DES-7200(config)#
```

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
service-policy	Associate one policy map to the specified interface.
mls qos map cos-exp	Map CoS value to the EXP value.
mls qos map exp-cos	Map CoS value to the EXP value.
show class-map	Display the specific contents of all class maps or the specified class map.
show policy-map	Display the specific contents of all policy maps or the specified policy map.

Platform description This command is supported by DES-7200 series devices based on EC line card.

3.2.9 set cos

Re-mark the CoS value of packets. Use **no** form of this command to disable re-marking.

set cos *new-cos* [**none-tos**]

no set cos

Parameter

Parameter	Description

description	*new-cos*	The new CoS value to be re-marked.
	none-tos	The DSCP value of packets is not modified while re-marking the CoS value of packets.

Default	NA
Command mode	Data classification configuration mode.
Usage guidelines	This command is used to re-mark the EXP value of topmost label of MPLS packets. When using this command, make sure the exp-cos and cos-exp maps use the default settings. Please refer to the configuration guidelines for detailed reasons.

Examples	Example: Configure all incoming MPLS packets on port Gi 1/1 with EXP value of topmost label being 2, so that the EXP value of topmost label will be re-marked to 1 after output.
	`DES-7200# configure terminal`
	`DES-7200(config)# class-map map1`
	`DES-7200(config-cmap)# match mpls experimental topmost 2`
	`DES-7200(config-cmap)# exit`
	`DES-7200(config)# policy-map policy1`
	`DES-7200(config-pmap)# class map1`
	`DES-7200(config-pmap-c)# set cos 1`
	`DES-7200(config-pmap-c)# exit`
	`DES-7200(config-pmap)# exit`
	`DES-7200(config)#`
	`DES-7200(config)# interface gigabitethernet 1/1`
	`DES-7200(config-if)# service-policy input policy1`
	`DES-7200(config-if)# exit`
	`DES-7200(config)#`

Related commands

Command	Description
class-map	Create a class map to identify objects and classify traffic as per certain matching rules.
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
service-policy	Associate one policy map to the specified interface.
mls qos map cos-exp	Map CoS value to the EXP value.
mls qos map exp-cos	Map CoS value to the EXP value.
show class-map	Display the specific contents of all class maps or the specified class map.
show policy-map	Display the specific contents of all policy maps or the specified policy map.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.3 Showing Related Commands

3.3.1 show class-map

Display the contents of class map.

show class-map [*class-name*]

Parameter description

Parameter	Description
class-name	Name of class map.

Default	Display all class maps.
Command mode	Privileged mode.
Usage guidelines	If the *class-name* is not specified, all class maps will be displayed. Enter the specific class-name to display contents of the specified class map.

Examples	Example: Configure one class-map to match multiple EXP values and display contents of this class-map.
	`DES-7200(config)# class-map map1`
	`DES-7200(config-cmap)# match mpls experimental topmost 1 2 3`
	`DES-7200(config-cmap)# exit`
	`DES-7200(config)# exit`
	`DES-7200# show class-map map1`
	
	`Class Map class1`
	`Match mpls experimental topmost 1 2 3`
	`DES-7200#`

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.

Platform description	Supported by DES-7200 series devices.

3.3.2 show mls qos interface

Display QoS information related to the interface.

show mls qos interface *interface-id* [**policers**]

Parameter description

Parameter	Description
interface-id	The interface to be displayed.
policers	Police associated to the interface.

Default

Display QoS information of all interfaces.

Command mode

Privileged mode.

Usage guidelines

If the *interface-id* is not specified, QoS information of all interfaces will be displayed; enter the specific interface-id to display the QoS information of the specified interface.

Examples

Example: Configure one policy map and associate to Gi 1/1 and display the QoS information of interface Gi 1/1.

```
DES-7200# configure terminal
DES-7200(config)# class-map map1
DES-7200(config-cmap)# match mpls experimental topmost 2
DES-7200(config-cmap)# exit
DES-7200(config)# policy-map policy1
DES-7200(config-pmap)# class map1
DES-7200(config-pmap-c)# set cos 1 none-tos
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
DES-7200(config)#
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# service-policy input policy1
DES-7200(config-if)# exit
DES-7200(config)# exit
DES-7200# show mls qos interface gigabitethernet 1/1
Interface: GigabitEthernet 1/1
```

```
Attached input  policy-map: policy1
Attached output policy-map:
Default trust: none
Default cos: 0
Attached mpls cos-exp group: 1
DES-7200#
```

Related commands

Command	Description
-	-

Platform description

Supported by DES-7200 series devices.

3.3.3 show mls qos maps

Display the cos-dscp maps, dscp-cos maps, ip-prec-dscp maps, cos-exp maps and exp-cos maps.

show mls qos maps [cos-dscp | dscp-cos | ip-prec-dscp | cos-exp | exp-cos]

Parameter description

Parameter	Description
cos-dscp	Display the cos-dscp maps.
dscp-cos	Display the dscp-cos maps.
ip-prec-dscp	Display the ip-prec-dscp maps.
cos-exp	Display the cos-exp maps.
exp-cos	Display the exp-cos maps.

Default

Display the cos-dscp maps, dscp-cos maps, ip-prec-dscp maps, cos-exp maps and exp-cos maps.

Command mode

Privileged mode.

Usage

If no map type is specified, all maps will be displayed.

guidelines

Examples

```
DES-7200# show mls qos maps exp-cos
exp cos
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
DES-7200#
DES-7200# show mls qos maps cos-exp
CoS-to-EXP Map group number: 1
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
   7  7
CoS-to-EXP Map group number: 2
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number: 3
```

```
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number：4
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number：5
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number：6
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
```

```
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number: 7
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number: 8
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
```

Related commands

Command	Description
-	-

Platform description

Displaying cos-exp maps and exp-cos maps is supported by DES-7200 series products based on EC line card.

3.3.4 show mls qos mpls

Display the MPLS QoS information.

show mls qos mpls

Parameter description

Parameter	Description
-	-

Default

NA

Command mode

Privileged mode.

Usage guidelines

NA

Examples

```
DES-7200# show mls qos mpls
Default mpls copy exp: disable
Default mpls propagate-exp none: disable
DES-7200#
```

Related commands

Command	Description
mpls copy experimental	Enable the MPLS EXP copying.
mpls propagate-experimental none	The EXP bits in the topmost label won't be copied to the second topmost label while removing the label stack.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.3.5 show policy-map

Display the contents of policy map (the specified class *class-name*).

show policy-map [*policy-name* [**class** *class-name*]]

Parameter description

Parameter	Description
policy-name	Name of policy name.
class-name	Name of class map.

Default

Display all policy names.

Command mode

Privileged mode.

Usage guidelines

If the policy-name is not specified, all policy maps will be displayed; enter the specific policy-name to display contents of the specified policy map. If the class-name is not specified, all class maps under the specified policy map will be displayed; if the specific class-name is specified, contents of this class map under the specified policy map will be displayed.

Examples

Example: Configure a policy map to configure all incoming MPLS packets with EXP value of topmost label being 2, so that the EXP value of topmost label will be marked to 1 after output. After configuring policy map, display the contents of this policy map.

```
DES-7200# configure terminal
DES-7200(config)# class-map map1
DES-7200(config-cmap)# match mpls experimental topmost 2
DES-7200(config-cmap)# exit
DES-7200(config)# policy-map policy1
DES-7200(config-pmap)# class map1
DES-7200(config-pmap-c)# set cos 1 none-tos
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
DES-7200(config)# exit
```

```
DES-7200# show policy-map policy1


 Policy Map policy1
     Class map1
       set cos 1 none-tos
DES-7200#
```

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
set cos	Re-mark the CoS value of packet.
show class-map	Display the specific contents of all class maps or the specified class map.

Platform description

Supported by DES-7200 series devices.

4 WRED Configuration Commands

4.1 Default Confiiugrations

	Parameter		Default Value	
Default configuration	Queue1	Threshold1	CoS	0，1，2，3，4，5，6，7
			WRED-drop	100%low，100%high
			random-detectprobability	60%
		Threshold2	CoS	NONE
			WRED-drop	80% low，100%high
			random-detectprobability	80%

Usage guidelines	By default, all wrr-queues are mapped to the threshold 1 of queue 1; the min-threshold value equals to the max-threshold and is 100%, representing the WRED function is disabled.

4.2 Related Configuration Commands

4.2.1 wrr-queue cos-map

Use this command to map the CoS value to a threshold for a specified queue in the interface configuration mode. Use the **no** form of this command to return to the default settings.

wrr-queue cos-map *threshold_id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]

Parameter description

Parameter	Description
queue_id	Interface queue id.

	cos_value	CoS value, in the range of 0-7

Default The cos value is the threshold for queue1.

Command mode Interface configuration mode.

Usage guidelines DSCP-threshold mapping can be enabled by mapping DSCP-CoS to CoS-threshold.

When all CoS values are mapped to one threshold on the interface, it changes the enabled WRED to RED.

Examples The following example shows how to set the cos1 and cos6 for queue2 (For the configuration of cos-queue mapping, use the **priority-queue cos-map** command in the global configuration mode.)

```
DES-7200(config-if)# wrr-queue cos-map 2 1 6
```

4.2.2 wrr-queue random-detect min-threshold

Use this command to set the minimum WRED threshold for the specified queue on the interface. Use the **no** form of this command to remove the minimum WRED threshold. The min-threshold value must be less than the max-threshold in the same group.

wrr-queue random-detect min-threshold *queue_id thr1* [*thr2 thr3*]

no wrr-queue random-detect min-threshold *queue_id*

Parameter description

Parameter	Description
queue_id	The interface queue id.
thr1	The min-threshold value for queue1.
thr2	The min-threshold value for queue2.
thr3	The min-threshold value for queue3.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines	Several physical ports could be in a WRED interface group, which requires for the completely-consistent WRED settings for those physical member ports. The related WRED parameters configured for one physical port are valid for other member ports in the same interface group. For DES-7200 series, each physical port corresponds to one interface group. DES-7200 series switches support to set the threshold for 2 queues only.
Examples	The following example shows how to set the min-threshold for queue1 on an interface: `DES-7200(config-if)# wrr-queuerandom-detect min-threshold 1 68 69 70`

4.2.3 wrr-queue random-detect probability

Use this command to set all maximum drop probability for the specified queue on the interface. Use the **no** form of this command to remove the maximum drop probability.

wrr-queue random-detect probability *queue_id prob1 [prob2 prob3]*

no wrr-queue random-detect probability *queue_id*

Parameter description

Parameter	Description
queue_id	The interface queue id.
prob1	The maximum drop probability for queue1.
prob2	The maximum drop probability for queue2.
prob3	The maximum drop probability for queue3.

Default	N/A.
Command mode	Interface configuration mode.
Usage guidelines	Several physical ports could be in a WRED interface group, which requires for the completely-consistent WRED settings for those physical member ports. The related WRED parameters configured for one physical port are valid for other member ports in the same interface group.

For DES-7200 series, each physical port corresponds to one interface group.

DES-7200 series support to set the maximum drop probability for 2 queues only.

Examples

The following example shows how to set the maximum drop probability for queue1 on an interface:

```
DES-7200(config-if)# wrr-queuerandom-detect probability
1 61 62 63
```

4.3 Showing Commands

4.3.1 show queueing wred interface

Use this command to show all WRED settings on an interface in the privileged user mode.

show queueing wred interface<*interface*>

Parameter description

Parameter	Description
interface	The physical interface number.

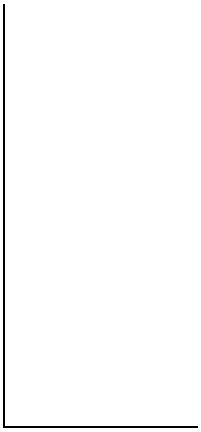
Command mode

Privileged user mode.

Examples

The following example shows the result of the command **show queueing wred interface g0/1**:

```
-----   -----   -----   ------   -----   -----   ------
qid max_1 min_1 prob_1 max_2 min_2 prob_2 max_3 min_3
prob_3
-----   -----   -----   ------   -----   -----   ------
1    0    0    90     0     0     91      0     0     92
2    88   66   90     87    55    91      86    66    92
3    0    0    0      0     0     0       0     0     0
4    0    0    0      0     0     0       0     0     0
5    88   66    0     89    67    0       90    68    0
6    0    0    0      0     0     0       0     0     0
7    0    0    0      0     0     0       0     0     0
8    0    0    0      0     0     0       0     0     0
cos  qid  threshold_id
```



| --- | --- | --- |
0	1	1
1	2	1
2	3	1
3	4	2
4	5	1
5	6	3
6	7	2
7	8	1

DES-7200

Reliability Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 VRRP Configuration Commands

1.1 Configuration Related Commands

1.1.1 vrrp accept_mode

Use this command to enable the packet accepting function on the IPv6 VRRP virtual router. The **no** form of this command is used to disable the function..

vrrp ipv6 *group* **accept_mode**

no vrrp ipv6 *group* **accept_mode**

Parameter description

Parameter	Description
group	VRRP group number

Default configuration

The master IPv6 VRRP is not allowed to accept packets whose destination IPv6 address is the IPv6 address of a virtual router. However, the NA and NS packets should be accepted regardless of the configuration of Accept_Mode. Also, the master IPv6 VRRP virtual router in the owner state will accept and process any packets whose destination IPv6 address is the IPv6 address of a virtual router, regardless of the configuration of Accept_Mode.

Command mode

Interface configuration mode.

Usage guidelines

Configuration of the network interface is effective for the master virtual router.

Caution

Only IPv6 VRRP has this configuration mode.

Examples

The example below enables the accept mode on the group 1:.

```
vrrp ipv6 1 accept_mode
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* ipv6 *ipaddress*	Enable VRRP and configure an IPv6 address for the virtual router.

Platform description

-

1.1.2 vrrp authentication

Use this command to enable VRRP authentication . The **no** format of this command disables the function.

vrrp *group* **authentication** *string*

no vrrp *group* **authentication**

Parameter description

Parameter	Description
group	VRRP group number
string	String for the VRRP group authentication (within 8 bytes, plaintext password)

Default configuration

By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, no authentication password is configured by default.

Command mode

Interface configuration mode.

Usage guidelines

The devices in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration.

Examples

The example below sets the authentication password for

	VRRP group 1. **vrrp** 1 **authentication** x30dn78k

Related commands	Command	Description
	DES-7200(config-if)# **vrrp** *group ip ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.

1.1.3 vrrp delay

Use this command to set the reload latency of the VRRP group on the interface.

vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

no vrrp delay

Parameter description	Parameter	Description
	min-seconds	When the interface is up, VRRP group shall be reloaded after at least min-seconds.
	reload-seconds	The reload latency of the VRRP group. If the configured min-seconds is more than reload-seconds, the actual reload latency of the VRRP group will be min-seconds.

Default configuration	By default, the VRRP reload delay function is not enabled on the interface.
Command mode	Interface configuration mode.
Usage guidelines	Use this command to set the reload latency of the VRRP group on the interface, when it is required that the VRRP group shall not be reloaded immediately after the system reloads or the interface is up. The reload latency range is 0-60.
Examples	The example below sets the VRRP reload latency on E0 to 10s. When E0 is up, VRRP group 1 shall be reloaded in 10s.

```
interface FastEthernet 0/0
shutdown
ip address 10.0.1.1 255.255.255.0
vrrp delay minimum 10
vrrp 1 ip 10.0.1.20
no shutdown
show vrrp 1
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.

1.1.4 vrrp description

Use this command to specify a descriptor for the VRRP. The **no** form of it restores it to the default.

vrrp *group* **description** *text*

no vrrp *group* **description**

Parameter description

Parameter	Description
group	VRRP group number
text	VRRP group descriptor

Default configuration

By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, no VRRP group descriptor is configured by default.

Command mode

Interface configuration mode.

Usage guidelines

This command will set the descriptor for the VRRP group to facilitate the identification of the VRRP group.

Examples

The example below labels the VRRP group 1 on Ethernet interface E0 as Building A – Marketing and Administration:

```
interface FastEthernet 0/0
ip address 10.0.1.1 255.255.255.0
```

```
vrrp 1 ip 10.0.1.20
vrrp 1 description “Building A - Marketing and
Administration”
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* ip *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device

1.1.5 vrrp ip

Use this command to enable VRRP on the interface and specify the related virtual IP address. The **no** format of the command disables the VRRP function and removes the setting of virtual IP address.

vrrp *group* **ip** *ipaddress* [**secondary**]

no vrrp *group* **ip** *ipaddress* [**secondary**]

Parameter description

Parameter	Description
group	VRRP group number of the virtual device
ipaddress	IP address of the virtual device
secondary	Specify the secondary IP address of the virtual device.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

If the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual device. Note that if the VRRP group is using the IP address of the Ethernet interface, an error occurs when you remove the IP address of the VRRP group with the **no** command, because there are duplicated IP address in the LAN.

Examples

The example below enables the VRRP function on Ethernet interface 0. The VRRP group number is 1,

primary IP address of the virtual device is 10.0.1.20 and secondary IP address is 10.0.2.20.

```
interface FastEthernet 0/0
no switchport// Used on the switch only.
ip address 10.0.1.1 255.255.255.0
ip address 10.0.2.1 255.255.255.0 secondary
vrrp 1 ip 10.0.1.20
vrrp 1 ip 10.0.2.20 secondary
```

Related commands

Command	Description
DES-7200# **show vrrp** [**brief | group**]	Show the VRRP configuration.

1.1.6 vrrp ipv6

Use this command to enable IPv6 VRRP on the interface and specify the related virtual IPv6 address. The **no** format of the command disables the IPv6 VRRP function and removes the setting of virtual IPv6 address.

vrrp *group* **ipv6** *ipv6-address*

no vrrp *group* **ip** *ipv6-address*

Parameter description

Parameter	Description
group	VRRP group number of the virtual device.
ipaddress	IPv6 address of the virtual device.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

IPv6 VRRP and IPv4 VRRP share group numbers ranging from 1 to 255. One VRRP group number of an interface is applicable to both IPv4 VRRP and IPv6 VRRP at the same time. The first configured address should be the link's local address, which cannot be deleted until the other virtual addresses are deleted.

Examples

The example below enables the IPv6 VRRP function on

Ethernet interface FastEthernet 0/0 with VRRP group number 1and virtual IPv6 address FE80::1 and 2001::1.

```
interface FastEthernet 0/0
no switchport
ipv6 enable
ip6 address 2001::2/64
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2001::1
```

Related commands

Command	Description
DES-7200# **show ipv6 vrrp** [**brief | group**]	Show the IPv6 VRRP configuration.

Platform description

Supported on all platforms.

1.1.7 vrrp preempt

Use this command to set the preemption mode of the VRRP group. The **no** command disables the VRRP preemption function.

vrrp *group* **preempt** [**delay** *seconds*]

no vrrp *group* **preempt**[**delay**]

Parameter description

Parameter	Description
group	VRRP group number
delay *seconds*	(Optional)Specify the delay before a device declares itself master. The default value is 0s.

Default configuration

By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

Command mode

Interface configuration mode.

Usage

If the VRRP group is working in the preemption mode,

guidelines

once a device finds its priority is higher than the priority of the master, it will become the master device of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the master's priority, it will not become the master device of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because that VRRP group has the highest priority and thus automatically becomes the master device in the VRRP group.

Examples

In the example below, once the VRRP group finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 s:

```
vrrp 1 preempt delay 15
vrrp 1 priority 200
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7200(config-if)# **vrrp** *group* **priority** *level*	Set the VRRP group priority.

1.1.8 vrrp priority

Use this command to specify the priority of the VRRP group. The **no** form of this command restores it to the default.

vrrp *group* **priority** *level*

no vrrp *group* **priority**

Parameter description

Parameter	Description
group	VRRP group number
level	VRRP group priority

Default configuration

By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

Command mode	Interface configuration mode.
Usage guidelines	None.
Examples	The example below sets the priority of VRRP group 1 as 254. `vrrp 1 priority 254`

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7200(config-if)# **vrrp** *group* **preempt** [**delay** *seconds*]	Set the VRRP in the preemption mode.

1.1.9 vrrp timers advertise

Use this command to specify the interval for the master device to send the VRRP advertisement. The **no** form of this command restores it to the default.

vrrp *group* **timers advertise** *interval*

no vrrp *group* **timers advertise**

Parameter description

Parameter	Description
group	VRRP group number
interval	Advertisement interval (in seconds)

Default configuration	By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the default advertisement interval of the master device is 1 second.
Command mode	Interface configuration mode.
Usage guidelines	If the current device becomes the master device in the VRRP group, it will notify its VRRP status, priority and

other information by sending the VRRP advertisement in the set interval.

Examples

The example below sets the VRRP advertisement interval as 4 seconds.

```
vrrp 1 timers advertise 4
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7200(config-if)# **vrrp group timers learn**	Enable the timer learning function.

1.1.10 vrrp timers learn

Use this command to enable the timer learning function. The **no** format of it disables the function.

vrrp *group* **timers learn**

no vrrp *group* **timers learn**

Parameter description

Parameter	Description
group	VRRP group number

Default configuration

By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, the timer learning function is disabled by default.

Command mode

Interface configuration mode.

Usage guidelines

Once the timer learning function is enabled, if the current device is a VRRP backup device, it will learn the VRRP advertisement interval from the VRRP advertisement of the master device, with which it calculates the master device's failure interval instead of the VRRP advertisement interval configured locally. This command may synchronize the VRRP advertisement timer with the master device.

Examples

The example below enables the timer learning function on the IPv4 VRRP group 1.

```
vrrp 1 timers learn
```

The example below enables the timer learning function on the IPv6 VRRP group 1.

```
vrrp ipv6 1 timers learn
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7200(config-if)# **vrrp** *group* **ipv6** *ipaddress*	Enable the VRRP function and set the IPv6 address for the virtual device.
DES-7200(config-if)# **vrrp** *group* **timers advertise** *interval*	Set the IPv4 VRRP advertising interval.
DES-7200(config-if)# **vrrp ipv6** *group* **timers advertise** *interval*	Set the IPv6 VRRP advertising interval.

1.1.11 vrrp track

Use the **vrrp** *group* **track** *interface-type number* command to enable the VRRP track in the interface configuration mode. Use the **vrrp** *group* **track** *ip_address* command to enable the VRRP IP address track. Use the **vrrp** *group* **track bfd** command to track the specified neighbor IP addrss via BFD. Use the **no** form of this command to disable this function.

vrrp *group* **track {***interface-type number* | **bfd** *interface-type number ipv4-address***}** [*priority*]

vrrp *group* **track** *ip-address* [[[**interval** *interval-value*] **timeout** *timeout-value*] *priority*]

vrrp *group* **track [***interface-type number* | **bfd** *interface-type number ipv4-address***]** [*ip-address*]

Parameter description

Parameter	Description
group	VRRP group number
interface-type	Type of monitored interface
number	Number of the monitored interface

Ipv4-address	Monitored IPv4 address. With BFD configured, it refers to the neighbor IP address.
interval-value	The interval of time to probe whether the monitored ip address is reachable or not. If this parameter is not selected, the default value is 3s.
timeout-value	The timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1s.
interface-priority	VRRP priority change range when the interface or ip address reachability status changes. If this parameter is not selected, the default value is 10.

Default configuration

By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, no interface or ip address is specified.

Command mode

Interface configuration mode.

Usage guidelines

This command can be used to monitor the outlet links. Note that layer-3 routable logical interfaces can be monitored (such as Routed Port, SVI, Loopback and Tunnel). This command can also be used to monitor the reachability of the specified IP address.

Examples

The example below enables the VRRP group 1 to monitor the routed port Fa1/1. If the Fa1/1 link is disconnected, the priority of the VRRP group decreases by 30. When the Fa1/1 link recovers, the priority of VRRP group 1 is restored.

```
vrrp 1 track FastEthernet 1/1 30
```

The example below shows how to set the VRRP to track the specified neighbor IP address 192.168.1.3 through BFD:

```
DES-7200#configure terminal
```

```
Enter configuration commands, one per line.  End with
CNTL/Z.
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#no switchport //used on the switch.
DES-7200(config-if)#ip address 192.168.1.1
255.255.255.0
DES-7200(config-if)#bfd interval 50 min_rx 50 multiplier
3
DES-7200(config)#interface FastEthernet 0/2
DES-7200(config-if)#no switchport  //used on the switch
DES-7200(config-if)#ip address 192.168.201.17
255.255.255.0

DES-7200(config-if)#vrrp 1 priority 120

DES-7200(config-if)#vrrp 1 ip 192.168.201.1
DES-7200(config-if)#vrrp 1 track bfd FastEthernet
0/1 192.168.1.3 30
DES-7200(config-if)#end
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7200(config-if)# **vrrp** *group* **priority** *level*	Set the VRRP group priority.

1.1.12 vrrp version

Use this command to configure the version of sending the IPv4 VRRP multicast packets. For the IPv4 VRRP, there are two version: VRRPv2 and VRRPv3.

vrrp *group* **version** {*2* | *3*}

no vrrp *group* **version**

Parameter description

Parameter	Description
2	Use the VRRPv2 version to send the packets.
3	Use the VRRPv3 version to send the packets.

Default configuration

VRRPv2.

Command mode	Interface configuration mode.
Usage guidelines	Considering the compatibility of VRRPv2 and VRRPv3 for the IPv4 VRRP, you can choose the version of VRRP packets based on the actual network environment. VRRPv2 is based on RFC3768 and VRRPv3 is based on RFC 5798. This command is applicable to IPv4 VRRP only.
Examples	The example below configures the version of sending the IPv4 VRRP packets on the interface gig4/1. `vrrp 1 version 3`

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7200(config-if)# **vrrp** *group* **timers advertise** *interval*	Set the interval of sending the VRRP advertisement.

1.2 VRRP Monitoring and Maintenance Commands

1.2.1 debug vrrp

Use this command to turn on the VRRP error prompt, VRRP event, VRRP message and status debug switches. The **no** form of this command turns off the switches.

debug vrrp

no debug vrrp

Default configuration	By default, the debug switches are turned off.
Command mode	Privileged mode.

Examples

In the example below, the user turns on the VRRP debug switch.

```
DES-7200# debug vrrp
DES-7200#
VRRP: Grp 1 Advertisement priority 120, ipaddr
192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Master
-> Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid
virtual address 192.168.1.1
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Backup
-> Master
DES-7200#
```

Related commands

Command	Description
DES-7200# **debug vrrp errors**	Turn on the VRRP error prompt debugging switch.
DES-7200# **debug vrrp events**	Turning on the VRRP event debugging switch.
DES-7200# **debug vrrp state**	Turning on the VRRP state debugging switch.

1.2.2 debug vrrp errors

Use this command to turn on the VRRP error prompt debug switch. The **no** form of this command turns off the switch.

debug vrrp errors

no debug vrrp errors

Default configuration By default, the VRRP error debug switch is turned off.

Command mode Privileged mode.

Examples

In the example below, the user turns on the VRRP error debug switch.

```
DES-7200# debug vrrp errors
DES-7200#
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid
virtual address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid
```

```
virtual address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid
virtual address 192.168.1.1
```

1.2.3 debug vrrp events

Use this command to turn on the VRRP event debug switch. The **no** form of this command turns off the switch.

debug vrrp events

no debug vrrp events

Default configuration	By default, the VRRP event debug switch is turned off.
Command mode	Privileged mode.
Examples	In the example below, the user turns on the VRRP event debug switch.

```
DES-7200# debug vrrp events
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
```

1.2.4 debug vrrp packets

Use this command to turn on the VRRP packet debug switch. The **no** form of this command turns off the switch.

debug vrrp packets

no debug vrrp packets

Default configuration	By default, the VRRP packet debug switch is turned off.
Command mode	Privileged mode.
Examples	In the example below, the user turns on the VRRP packet debug switch, where the checksum of the packets of VRRP group 1 is displayed.

```
DES-7200# debug vrrp packets
DES-7200#
VRRP: Grp 2 sending Advertisement checksum DD4D
```

```
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
```

In the example below, the user turns on the VRRP packet debug switch, where the source IP address of the VRRP group 1 packets and the priority of VRRP group 1 are displayed.

```
DES-7200# debug vrrp packets
DES-7200#
VRRP: Grp 1 Advertisement priority 120, ipaddr
192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr
192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr
192.168.201.213
```

1.2.5 debug vrrp state

Use this command to turn on the VRRP status debug switch. The **no** form of this command turns off the switch.

debug vrrp state

no debug vrrp state

Default configuration	By default, the VRRP debug switch is turned off.
Command mode	Privilege mode.

Examples

In the example below, the user turns on the VRRP status debug switch.

```
DES-7200# debug vrrp state
DES-7200#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master
-> Backup
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Backup
-> Master
DES-7200# config terminal
Enter configuration commands, one per line. End with
CNTL/Z.
DES-7200(config)# interface fastethernet 0/0
DES-7200(config-if)#no shutdown
DES-7200(config-if)# end
DES-7200#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master
-> Init
```

1.3 Showing Related Command

1.3.1 show vrrp

Use this command to show the VRRP information.

show vrrp [**brief** | *group*]

Parameter description

Parameter	Description
brief	(Optional) Show the brief of the VRRP group.
group	Number of the VRRP group to be displayed

Command mode

Privileged mode.

Usage guidelines

If no optional parameter is used, the information of all VRRP groups is displayed.

Examples

Show the information of all VRRP groups:

```
DES-7200# show vrrp
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
DES-7200#
```

Show the brief information of the VRRP group:

```
DES-7200# show vrrp brief
Interface    Grp Pri Time  Own Pre State   Master addr   Group addr
FastEthernet 0/0  1  100   -  -  P  Backup  192.168.201.213 192.168.201.1
FastEthernet 0/0  2  120   -  -  P  Master  192.168.201.217 192.168.201.2
DES-7200#
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group ip ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.

1.3.2 show vrrp interface

Use this command to show the information of the VRRP on the interface.

show vrrp interface *type number* [**brief**]

Parameter description

Parameter	Description
type	Interface type
number	Interface number
brief	(Optional) Show the brief of the VRRP group on the interface.

Command mode

Privileged mode.

Examples

The example below shows the VRRP information on Ethernet interface E1/0

```
DES-7200# show vrrp interface fastethernet 0/0
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
```

```
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
```

Related commands

Command	Description
DES-7200(config-if)# **vrrp** *group* **ip** *ip address* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device

1.3.3 show vrrp packets statistics

Use this command to show the statistics of the VRRP packets transmission.

show vrrp packet statistics [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and number.

Command mode

Privileged mode.

Examples

N/A

Related commands

Command	Description
-	-

2 VRRP Plus Configuration Commands

2.1 Configuration Related Command

2.1.1 vrrp balance

Use this command to enable the VRRP Plus function. Use the **no** form of this command to disable this function.

vrrp *group* **balance**

no vrrp *group* **balance**

Parameter description

Parameter	Description
group	Enable the VRRP Plus function on the VRRP of specified group ID.

Default Disabled.

Command mode Interface configuration mode.

Usage guidelines The VRRP function should be configured before enabling the VRRP Plus function.

Examples The following example enables the VRRP Plus function on the layer3 interface FastEthernet0/0.

```
interface FastEthernet 0/0
vrrp 1 ip 192.168.1.1
vrrp 1 balance
```

Related

Command	Description

	vrrp *group* **load-balancing** { **host-dependent** | **round-robin** | **weighted** }}	Set the load balancing policy of the VRRP Plus.
	show vrrp balance [**brief** | *group*]	Show the VRRP Plus running status.
	show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status of the specified interface.

2.1.2 vrrp forwarder preempt

Use this command to enable the forwarding preemption on the VRRP Plus backup group. Use the **no** form of this command to disable this function. .

vrrp *group* **forwarder preempt**

no vrrp *group* **forwarder preempt**

Parameter description

Parameter	Description
group	Enable the forwarding preemption function on the VRRP Plus backup group of specified group ID.

Default Enabled.

Command mode Global configuration mode.

Usage guidelines The VRRP Plus function should be configured before enabling the forwarding preemption.

Examples The following example enables the forwarding preemption function of the VRRP Plus backup group on the layer3 interface FastEthernet0/0.

```
interface FastEthernet 0/0
vrrp 1 ip 192.168.1.1
vrrp 1 balance
vrrp 1 forwarder preempt
```

Related commands

Command	Description
vrrp *group* **balance**	Enable the VRRP Plus function.
show vrrp balance [**brief** | *group*]	Show the VRRP Plus running status.
show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status of the specified interface.

2.1.3 vrrp load-balancing

Use this command to set the VRRP Plus load balancing policy. Use the **no** form of this command to restore it to the default setting.

vrrp *group* **load-balancing** { **host-dependent | round-robin** | **weighted** }

no vrrp *group* **load-balancing** { **host-dependent | round-robin** | **weighted** }

Parameter description

Parameter	Description
group	Specify the VRRP group ID.
host-dependent	Set the host-dependent load balancing policy, so as to use the different virtual MACs to reply the host's ARP request based on different hosts.
round-robin	Set the round-robin balancing policy, so as to use the different virtual MACs to reply the host's ARP request in turn, which is the default setting.
weighted	Set the weight balancing policy, so as to perform the ARP reply based on the device weight of the backup group.

Default Round-robin.

Command mode Interface configuration mode.

Usage guidelines The VRRP Plus function should be enabled before setting the VRRP Plus load balancing policy.

Examples The following example sets the load balancing policy of the VRRP Plus group1 as the host-dependent.

```
DES-7200(config-if)# vrrp 1 ip 192.168.1.1
DES-7200(config-if)# vrrp 1 balance
DES-7200(config-if)# vrrp 1 load-balancing host-dependent
```

Related commands

Command	Description
vrrp *group* **balance**	Enable the VRRP Plus function.
show vrrp balance [**brief** | *group*]	Show the VRRP Plus running status.
show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status o the specified interface.

2.1.4 vrrp timers redirect

Use this command to set the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group. Use the **no** form of this command to restore the redirection interval and timeout to the default value.

vrrp *group* **timers redirect** *redirect timeout*

no vrrp *group* **timers redirect**

Parameter description

Parameter	Description
group	VRRP Plus backup group ID, in the range of 1 to 255.
redirect	The redirection time, 300 seconds (namely 5 minutes) by default, in the range of 0 to 3600.
timeout	The timeout, 14400 seconds (namely 4 hours) by default, in the range of (redirect+600) to 64800.

Default

Redirection interval: 300 seconds, redirection timeout: 14400 seconds.

Command mode

Interface configuration mode.

Usage guidelines	The VRRP Plus function should be enabled before setting the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group.

Examples

```
DES-7200(config-if)# vrrp 1 ip 192.168.1.1
DES-7200(config-if)# vrrp 1 balance
DES-7200(config-if)# vrrp 1 timers redirect 300 6000
```

Related commands

Command	Description
vrrp *group* **balance**	Enable the VRRP Plus function.
show vrrp balance [**brief** | *group*]	Show the VRRP Plus running status.
show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status o the specified interface.

2.1.5 vrrp weighting

Use this command to set the weight and threshold of the VRPP Plus backup group. Use the **no** form of this command to restore the two values to default.

vrrp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]

no vrrp *group* **weighting**

Parameter description

Parameter	Description
group	VRRP Plus backup group ID, in the range of 1 to 255.
maximum	Weight, 100 by default, in the range of 1 to 254.
lower	Weight lower, 1 by default, in the range of 1 to (maximum-1)
upper	Weight upper, 100 by default, in the range of lower to maximum.

Default

VRRP Plus backup group weight: 100.
Weight lower: 1.
Weight upper: 100.

Command mode	Interface configuration mode.

Usage guidelines	The VRRP Plus function should be enabled before setting the weight and threshold of the VRRP Plus backup group.

Examples

The following example sets the weight and threshold of the VRRP Plus group1.

```
DES-7200(config-if)# vrrp 1 ip 192.168.1.1
DES-7200(config-if)# vrrp 1 balance
DES-7200(config-if)# vrrp 1 weighting 50 lower 30 upper 50
```

Related commands

Command	Description
vrrp *group* **balance**	Enable the VRRP Plus function.
show vrrp balance [**brief** | *group*]	Show the VRRP Plus running status.
show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status of the specified interface.

2.1.6 vrrp weighting track

Use this command to set the track object corresponding to the weight of the VRRP Plus backup group. Use the **no** form of this command to delete the corresponding track object.

vrrp *group* **weighting track** *object-number* [**decrement** *value*]

no vrrp *group* **weighting track** *object-number*

Parameter description

Parameter	Description
group	VRRP Plus backup group ID, in the range of 1 to 255.
object-number	The ID of the track object created by the track module, in the range of 1 to 700.
value	Weight decrement performed when the track object is down, which is 10 by default and is in the 1 to 255.

Default	No track is configured by default.

Command mode	Interface configuration mode.
Usage guidelines	The VRRP Plus function should be enabled before setting the track object corresponding to the weight of the VRRP Plus backup group..
Examples	DES-7200(config)#track 1 interface gigabitEthernet 0/14 line-protocol DES-7200(config-if)# **vrrp** *1* **ip** *192.168.1.1* DES-7200(config-if)# **vrrp** *1* **balance** DES-7200(config-if)# **vrrp** *1* **weighting track** *1* **decrement** *50*

Related commands

Command	Description
vrrp *group* **balance**	Enable the VRRP Plus function.
show vrrp balance [**brief** | *group*]	Show the VRRP Plus running status.
show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status of the specified interface.

2.2 Monitoring and maintenance Related Commands

2.2.1 debug vrrp balance

The VRRP Plus module is added the following debugging switch:

- **debug vrrp balance errors**, which is used to monitor the errors.
- **debug vrrp balance messages**, which is used to monitor the messages between the VRRP and TRACK modules.
- **debug vrrp balance packets**, which is used to monitor the VRRP Plus protocol packets.
- **debug vrrp balance state**, which is used to monitor the VRRP Plus group state.
- **debug vrrp balance timer**, which is used to monitor the VRRP Plus group timer.

- **debug vrrp balance event**, which is used to monitor the VRRP Plus group events.
- **debug vrrp balance**, which is used to monitor all information.

2.2.2 show vrrp balance

1.2.2.1 show vrrp balance interface

Use this command to show the actions of the VRRP Plus group on the specified interface .

show vrrp balance interface *type number* [**brief**]

Parameter description

Parameter	Description
interface *type number*	Specify the interface type and number.
brief	(Optional) show the brief information.

Default -

Command mode Privileged mode.

Usage guidelines -

Examples

The following example shows the actions of the VRRP Plus on FastEthernet 0/0.

```
DES-7200# show vrrp balance interface FastEthernet 0/0
FastEthernet 0/0 - Group 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 90 (configured 100), thresholds: lower 1,
   upper 100
    Track object 1, state: down, decrement weight: 10
  There are 2 forwarders
  Forwarder 1 (local)
```

```
    MAC address:
      0000.5e00.0101
    Owner ID is 00d0.f822.33ab
  Forwarder 2
    MAC address:
      001a.a916.0201
    Owner ID is 00d0.f822.8800
```

Related commands

Command	Description
vrrp *group* **balance**	Enable the VRRP Plus function.
vrrp *group* **load-balancing** { **host-dependent** | **round-robin** | **weighted**}	Set the load balancing policy of the VRRP Plus.
show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status of the specified interface.

1.2.2.2 show vrrp balance

Use this command to show the VRRP Plus brief or details .

show vrrp balance [**brief** | *group*]

Parameter description

Parameter	Description
brief	(Optional) show the VRRP Plus brief.
group	(Optional) show the VRRP Plus details.

Default NA

Command mode Privileged mode.

Usage guidelines If no optional parameter is used, the details of all VRRP Plus group are shown.

Examples The following example shows the details of all VRRP Plus

groups.

```
DES-7200#show vrrp balance
VLAN 1 - Group 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 90 (configured 100), thresholds: lower 1,
  upper 100
    Track object 1, state: down, decrement weight: 10
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
    Owner ID is 00d0.f822.33ab
  Forwarder 2
    MAC address:
      001a.a916.0201
    Owner ID is 00d0.f822.8800
```

The following example shows the brief of the VRRP Plus group.

```
DES-7200# show vrrp balance brief
Interface  Grp   State     Group Addr      MAC addr
VLAN 1       1    BVG    192.168.1.1     0000.5e00.0101
```

Related commands

Command	Description
vrrp *group* **balance**	Enable the VRRP Plus function.
vrrp *group* **load-balancing** { **host-dependent** | **round-robin** | **weighted**}	Set the load balancing policy of the VRRP Plus.
show vrrp balance interface *type number* [**brief**]	Show the VRRP Plus running status of the specified interface.

3 BFD Configuration Commands

3.1 Related Configuration Commands

3.1.1 bfd

Use this command to set the BFD session parameter in the interface configuration mode. Use the **no** form of this command to remove the setting.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

no bfd interval

Parameter description

Parameter	Description
interval *milliseconds*	Interval of sending the BFD control messages to the BFD session neighbor. *milliseconds:* valid range from 50ms to 10000ms.
min_rx *milliseconds*	Expected interval of receiving the BFD control messages from the BFD session neighbor. *milliseconds:* valid range from 50ms to 10000ms.
multiplier *multiplier-value*	Count of BFD control message not received from the peer in the configured interval. *multiplier-value::* valid range from 3 to 50.

Default No BFD session parameters by default. Those parameters must be configured before enabling the BFD session.

Command mode Interface configuration mode.

Usage guidelines	Note that this command is not configurable on the L3 AP. The express forwarding must be enabled before enabling BFD on the routers.

Examples	The following example shows how to configure the BFD session parameter on Routed Port FastEthernet 0/2:
	`DES-7200(config)# interface fastEthernet 0/2`
	`DES-7200(config)# no switchport`
	`DES-7200(config-if)# bfd interval 100 min_rx 100 multiplier 3`

Related commands

Command	Description
bfd all-interfaces	Configure BFD for all route protocols on the interface.
clear bfd	Clear the BFD session statistics.
ip ospf bfd	Configure BFD for OSPF.
ip rip bfd	Configure BFD for RIP.

3.1.2 bfd all-interfaces

Use this command to configure the BFD for the route protocols in the (RIP, OSPF)router configuration mode. Use the **no** form of this command to disable this function.

bfd all-interfaces

no bfd all-interfaces

Parameter description

Parameter	Description
-	-

Default	By default, BFD can not be configured for all route protocols on the interface.
Command mode	Route configuration mode.
Usage guidelines	Use the following two methods to enable or disable the BFD configuration for route protocols on the interface:

1. Use the **[no] bfd all-interfaces** command in the OSPF and RIP route configuration mode;
2. Use the **ip ospf bfd** [**disable**] or **ip rip bfd** [**disable**] command in the interface configuration mode.

Examples

The following example shows how to configure the BFD for OSPF on alll interfaces:

```
DES-7200(config)# router ospf 123
DES-7200(config-router)# bfd all-interfaces
```

Related commands

Command	Description
bfd	Configure the BFD session parameter.
ip ospf bfd	Configure the BFD for OSPF.
ip rip bfd	Configure the BFD for RIP.

3.1.3 bfd cpp

Use this command to enable the BFD protection policy in the global configuration command. Use the **no** form of this command to disable BFD CPP.

bfd cpp

no bfd cpp

Parameter description

Parameter	Description
-	-

Default

Enabled.

Command mode

Global configuration mode.

Usage guidelines

BFD protocol is so sensitive that if the device with BFD function enabled suffers from attack (for example, a large amount of Ping packets attack the device), which lead to the BFD session turbulence, the device can be protected by enabling the BFD protection policy. However, if the BFD function and the BFD protection policy are enabled at the same time, the loss of BFD packets on the attacked device

	occurs when the packets sent from the last-hop device go through this device, influencing the BFD session establishment between the last-hop device and other devices. This function is valid only for the switches.
Examples	The following example shows how to enable the BFD protection policy: `DES-7200(config)# bfd cpp`

Related commands

Command	Description
-	-

3.1.4 bfd echo

Use this command to enable the echo mode in the interface configuration mode. Use the **no** form of this command to disable this function.

bfd echo

no bfd echo

Parameter description

Parameter	Description
-	-

Default	Enbaled
Command mode	Interface configuration mode.
Usage guidelines	By default, with BFD session parameter configured, the system enables the echo mode automatically. The minimum sending and receiving interval for the echo packets are the values of the configured **interval** *milliseconds* and **min_rx** *milliseconds.*

	 **Caution** This command can not be configured on the L3 AP port. Before enabling BFD ECHO mode, it is necessary to use the **no ip redirects** command to disable the ICMP redirection messages sending on the neighbor device of the BFD session, use the **no ip deny land** to disable the DDOS(Land-based attack prevention) function. With both ends of the BFD session enabled, the Echo mode takes effect.

Examples

The example below shows how to set the echo mode on the Routed Port FastEthernet 0/2:

```
DES-7200(config)# interface fastEthernet 0/2
DES-7200(config)# no switchport
DES-7200(config-if)# bfd echo
```

Related commands

Command	Description
bfd	Configure the BFD session parameter.
ip redirects	Enable the ICMP message redirection function.
bfd slow-timer	Configure the slow-timer time.

3.1.5 bfd slow-timer

Use this command to enable the BFD ECHO function and set the slow timer, which is used to send the BFD control packets in the BFD asynchronous mode in the global configuration mode. Use the **no** form of this command to return to the default value.

bfd slow-timer *milliseconds*

no bfd slow-timer

Parameter description

Parameter	Description
milliseconds	BFD slow-timer time, in ms. In the range of 1000-30000, the default value is 1000ms.

Default	1000ms.
Command mode	Global configuration mode.
Usage guidelines	-
Examples	The example below sets the slow-timer as 14000ms: `DES-7200(config)# bfd slow-timer 14000`

Related commands

Command	Description
bfd echo	Enable the BFD echo function

3.1.6 bfd up-dampening

Use this command to set the bfd up-dampening time. Use the **no** form of this command to return to the default value.

bfd up-dampening [*milliseconds***]**

no up-dampening

Parameter description

Parameter	Description
milliseconds	(Optional) Set the bfd up-dampening time, in ms. In the range of 0-300000.

Default	0ms, which means that the session state is UP and notifying the application leval of the state change immediately.
Command mode	Interface configuration mode.
Usage guidelines	-
Examples	The example below sets the bfd up-dampening time as 60000ms: `DES-7200(config)# bfd up-dampening 60000`

Related commands

Command	Description
bfd	Configure the BFD session parameter.

3.1.7 bfd bind peer-ip

Use this command to create a bfd session to co-operate with one interface status in this interface configuration mode. Use the **no** form of this command to remove this session.

bfd bind peer-ip *ip-address* [**source-ip** *ip-address*] **process-pst**

no bfd bind peer-ip *ip-address*

Parameter description

Parameter	Description
peer-ip *ip-address*	The peer IP address to be detected, which must directly-connect to the Layer-3 interface.
source-ip *ip-address*	Source IPaddress for sending the BFD packets, which avoids the packets dropped by the URPF in case that this function is used with other functions such the URPF at the same time.
process-pst	Associate this session with the bdf status of the Layer-3 interface.

Default None

Command mode Interface configuration mode.

Usage guidelines Note that this command must be configured on the Layer-3 interface and the peer-ip detected must be the address directly-connected to the interface.

Examples The example below detects the peer 1.1.1.2 through BFD on the routed port to generate the BFD status of the

interface.

```
DES-7200(config)# interface FastEthernet 0/2
DES-7200(config-if)#no sw
DES-7200(config-if)#ip address 1.1.1.1 255.255.255.0
DES-7200(config-if)#bfd bind peer-ip 1.1.1.2 source-ip
1.1.1.1 process-pst
```

Related commands

Command	Description
-	-

3.1.8 ip ospf bfd

Use this command to configure the BFD for OSPF in the interface configuration mode. Use the **no** form of this command to remove this configuration.

ip ospf bfd [**disable**]

no ip ospf bfd [**disable**]

Parameter description

Parameter	Description
disable	(Optional) Disable the configuration of BFD for OSPF on the interface.

Default

Enabled if the keyword **disable** is not input.

Command mode

Interface configuration mode.

Usage guidelines

The following two methods are used to enable or disable the configuration of BFD for OSPF:

1. Use the **[no] bfd all-interfaces** command to enable or disable the configuration of BFD for the routing protocols on all interfaces in the OSPF routing configuration mode.

2. Use the **ip ospf bfd [disable]** command to enable or disable the configuration of BFD for OSPF on the specified interface in the interface configuration mode.

Examples

The example below shows how to disable the configuration of BFD for OSPF on the Routed Port FastEthernet 0/2:

```
DES-7200(config)# interface FastEthernet 0/2
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip ospf bfd disable
```

Related commands

Command	Description
bfd	Set the BFD session parameters.
bfd all-interfaces	Configure the BFD for the routing protocols on all interfaces.

3.1.9 ip rip bfd

Use this command to configure the BFD for RIP in the interface configuration mode. Use the **no** form of this command to remove this configuration.

ip rip bfd [**disable**]

no ip rip bfd

Parameter description

Parameter	Description
disable	(Optional) Disable the configuration of BFD for RIP on the interface.

Default

Enabled if the keyword **disable** is not input.

Command mode

Interface configuration mode.

Usage guidelines

The following two methods are used to enable or disable the configuration of BFD for RIP:

1. Use the **[no] bfd all-interfaces** command to enable or disable the configuration of BFD for the routing protocols on all interfaces in the RIP routing configuration mode.

2. Use the **ip rip bfd [disable]** command to enable or disable the configuration of BFD for RIP on the specified interface in the interface configuration mode.

Examples

The example below shows how to disable the configuration of BFD for RIP on the Routed Port FastEthernet 0/2:

```
DES-7200(config)# interface FastEthernet 0/2
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip rip bfd disable
```

Related commands

Command	Description
bfd	Set the BFD session parameters.
bfd all-interfaces	Configure the BFD for the routing protocols on all interfaces.

3.1.10 ip route static bfd

Use this command to configure the BFD for the static route in the global configuration mode. Use the **no** form of this command to remove this configuration.

ip route static bfd [vrf *vrf-name***] i***nterface-type interface-number* **gateway [***source ip-address***]**

no ip route static bfd [vrf *vrf-name***]** *interface-type interface-number* **gateway [***source ip-address***]**

Parameter description

Parameter	Description
vrf *vrf-name*	(Optional) set the VRF name of the static router.
interface-type interface-number	Set the interface type and interface number.
gateway	Set the IP address for the gateway, which is the neighbor IP address for BFD. The static route next-hop of the neighbor detects the reachability of the forwarding path through BFD.
source *ip-address*	(Optional) set the source IP address for the BFD session. It is necessary to set this parameter if the distance between the session IP address and the neighbor IP address are multi-hops.

Default No configuration of BFD for the static route.

Command mode	Global configuration mode.
Usage guidelines	Note that the BFD session parameters must have been configured before the configuraiton.

Examples	The example below shows how to configure the BFD for the static routes and detects the forwarding path between the neighbor 172.16.0.2 through BFD:
	`DES-7200(config)# interface FastEthernet 0/1`
	`DES-7200(config-if)# no switchport`
	`DES-7200(config-if)# ip address 172.16.0.1 255.255.255.0`
	`DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3`
	`DES-7200(config)# ip route static bfd FastEthernet 0/1 172.16.0.2`
	`DES-7200(config)# ip route 10.0.0.0 255.0.0.0 FastEthernet 0/1 172.16.0.2`

Related commands

Command	Description
bfd	Set the BFD session parameters.

3.1.11 neighbor fall-over bfd

Use this command to configure the BFD for BGP and detects the change of the specified neighbor to speed up the BGP convergence in the route or addres-family configuration mode. Use the **no** form of this command to disable this function.

neighbor *ip-address* **fall-over bfd**

no neighbor *ip-address* **fall-over bfd**

Parameter description

Parameter	Description
ip-address	Specify the BGP neighbor.

Default	No configuration of BFD for BGP.

Command mode	Route or address-family configuration mode.
Usage guidelines	Note that the BFD session parameters must have been configured before the configuraiton.

Examples	The example below shows how to configure the BFD for BGP and detects the forwarding path between the neighbor 172.16.0.2 through BFD:
	`DES-7200(config)# routerbgp 44000`
	`DES-7200(config-router)# bgp log-neighbors-changes`
	`DES-7200(config-router)# neighbor 172.16.0.2 remote-as 45000`
	`DES-7200(config-router)# neighbor 172.16.0.2 fall-over bfd`
	`DES-7200(config-router)# end`

Related commands

Command	Description
bfd	Set the BFD session parameters.

3.1.12 set ip next-hop verify-avalability

Use this command to configure the BFD for PBR and detects whether the next-hop of the configured PBR is valid or not by the Track method. Use the **no** form of this command to disable this function.

set ip next-hop verify-availability next-hop-address {**track** number **|bfd** [**vrf** vrf-name] interface-type interface-number gateway}

no set ip next-hop verify-availability next-hop-address {**track** number |**bfd** [**vrf** vrf-name] interface-type interface-number gateway}

Parameter description

Parameter	Description
vrf *vrf-name*	Set the VRF name of the static router.
next-hop-address	Set the next-hop IP address.
track	Determine whether the next-hop is valid or not by the Track method.
number	The track object number.
bfd	Neighbor detection by the

	BFD method.
interface-type interface-number	Set the interface type and interface number.
gateway	Set the IP address for the gateway, which is the neighbor IP address for BFD. The static route next-hop of the neighbor detects the reachability of the forwarding path through BFD.

Default

No configuration of BFD for PBR.

Command mode

Route-map configuration mode.

Usage guidelines

Note that the BFD session parameters must have been configured before the configuraiton.

Examples

The example below shows how to configure the BFD for PBR and detects the forwarding path between the neighbor 172.16.0.2 through BFD:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# route-map Example1 permit 10
DES-7200(config-route-map)# match ip address 1
DES-7200(config-route-map)# set ip precedence priority
DES-7200(config-route-map)#set ip next-hop verify-availability 172.16.0.2 bfd FastEthernet 0/1 172.16.0.2
DES-7200(config-route-map)#end
```

Related commands

Command	Description
bfd	Set the BFD session parameters.

3.1.13 vrrp bfd

Use this command to configure the BFD for VRRP and detects whether the master router is active or not in the interface configuration mode. Use the **no** form of this command to disable this function.

vrrp group-number **bfd** ip-address

no vrrp group-number **bfd** ip-address

Parameter description

Parameter	Description
group-number	Configure the BFD for the specified VRRP group to detect whether the master router is active or not.
Ip-address	Specify the neighbor IP address.

Default

By default, VRRP does not detect whether the master or backup router is active or not through BFD.

Command mode

Interface configuration mode.

Usage guidelines

Note that the BFD session parameters must have been configured before the configuraiton.

If multiple routers exist in the VRRP group, it is a necessity to use this command to set the neighbor IP address for all possible backup routers.

Examples

The example below shows how to configure the BFD for VRRP and detects the forwarding path between the master and backup routers through BFD:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.201.11 255.255.255.0
DES-7200(config-if)#bfd interval 50 min_rx 50 multiplier 3 DES-7200(config-if)#vrrp 1 priority 120
```

```
DES-7200(config-if)#vrrp 1 ip 192.168.201.1
DES-7200(config-if)#vrrp 1 bfd 192.168.201.12
DES-7200(config-if)#end
```

Related commands

Command	Description
bfd	Set the BFD session parameters.

3.2 Showing and Monitoring Commands

3.2.1 show bfd neighbors

Use this command to show the BFD session parameters.

show bfd neighbors [**vrf** *vrf-name*] [**client** { **bgp | ospf | rip | vrrp | static-route | vrrp-balance | ldp-lsp | static-lsp | backward-lsp-with-ip | pst**}] [**ipv4** *ip-addess* | **ipv6** *ip-addess*] [**details**]

Parameter description

Parameter	Description
vrf *vrf-name*	(Optional) set the neighbor VRF name.
client	(Optional) specify the routing protocol.
bgp	Show the BFD session configuration for BGP.
ospf	Show the BFD session configuration for OSPF.
rip	Show the BFD session configuration for RIP.
vrrp	Show the BFD session configuration for VRRP.
static-route	Show the BFD session configuration for the static route.
pbr	Show the BFD session configuration for PBR.
vrrp-balance	Show the BFD session configuration for the VRPP.
ldp-lsp	Show the BFD session configuration for the

	LDP-LSP.
backward-lsp-with-ip	Show the BFD session configuration for the LSP backward IP co-operation.
static-lsp	Show the BFD session configuration for the static LSP co-operation.
pst	Show the BFD session configuraiton and the layer-3 interface status.
ipv4 *ip-address*	(Optional) Show the session information of the specified IPv4 neighbor.
ipv6 *ip-address*	(Optional) Show the session information of the specified IPv6 neighbor.
details	(Optional) Show the configurations in detail.

Command mode

Privileged EXEC mode.

Usage guidelines

In the release 10.4(3), the ldp-lsp, static-lsp and backward-lsp-with-ip are not supported by routers, but only supported by DES-7200 series.

Examples

#The following shows the result of the command **show bfd neighbors**:

```
DES-7200# show bfd neighbors
 OurAddr   NeighAddr  LD/RD RH  Holdown(mult)  State
    Int
172.16.11.1 172.16.11.2 1/2   1    532 (3 )  Up
    Ge2/1
```

#The following shows the result of the command **show bfd neighbors details**:

```
DES-7200# show bfd neighbors details
OurAddr   NeighAddr   LD/RD RH Holdown(mult) State
    Int
172.16.11.1 172.16.11.2 1/2   1    532 (3 )  Up
    Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg:
208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg:
152/248/196 Registered protocols: BGP
Uptime: 02:18:49
Last packet:     Version: 1               -
Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0                  - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2             - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0
```

Field	Descripton
OurAddr	Local IP address.
NeighAddr	Neighbor IP address.
LD/RD	Local & Remote identifiers.
RH/RS	Whether the remote session responses the local session.
Holdown(mult)	Time of not receiving the hello packets for the local session and the times of the timeout detection.
State	The current session state.
Int	The interface number for the session.

Session state is UP and using echo function with 50 ms interval	Whether the session is in the echo mode and the echo interval (which is shown only in the echo mode).
Local Diag	Session diagnostic information.
Demand mode	Whether the session poll mode is active or not.
Poll bit	Whether the session configuration has been modified or not.
MinTxInt	The minimum sending interval for the local session.
MinRxInt	The minimum receiving interval for the local session.
Multiplier	The timeout detection times for the local session.
Received MinRxInt	The minimum sending interval for the remote session.
Received Multiplier	The timeout detection times for the remote session.
Holdown (hits)	The session detection time and the times of the timeout detection.
Hello (hits)	The minimium interval of receiving the hello packets after the session negotiation.
Rx Count	The number of BFD packets received by the local session.
Rx Interval (ms) min/max/avg	The minimum, maximum and average intervals of receiving for the local session.

Tx Count	The number of BFD packets sent by the local session.
Tx Interval (ms) min/max/avg	The minimum, maximum and average intervals of sending for the local session.
Registered protocols	The registered protocol type of the session.
Uptime	The time of keeping the session UP.
Last packet	The last BFD packet information received by the local session.

4 DLDP Configuration Commands

4.1 Configuration Related Commands

4.1.1 dldp ip

Use this command to enable the DLDP detection function. Use the **no** form of this command to disable the DLDP detection function for the specified IP address.

dldp *ip* **[***nexthopip***] [interval** *interval-value* **| retry** *retry-value***| resume** *resume-value***]**

no dldp *ip* **[***nexthopip***]**

Parameter description

Parameter	Description
ip	The peer IP address
nexthopip	The nexthop IP address
interval-value	The detection interval time. The valid range is 1-3600, in ticket, 1 ticket≈10ms
retry-value	The retransmission times. The valid range is 1-3600.
resume-value	The resume times of the link of the peer device detected. Before changing the link state from DOWN to UP, the continuous DLDP detection packets shall be received. The valid range is 1-200.

Default configuration

Interval:100ms;

Retry:3;

Working mode: passive mode;

Resume: 1.

Command mode	Interface configuration mode.
Usage guidelines	Use this command to enable the DLDP detection function for the rapid detection of the Ethernet link error.

Examples	**Example 1:** enable the DLDP function for the device 10.83.132.10:
	`DES-7200(config)# interface fastethernet 1/0`
	`DES-7200(config-if)# dldp 10.83.132.1`
	`DES-7200(config-if)#`
	
	Example 2: enable the DLDP function in the passive mode:
	`DES-7200(config-if)# dldp passive.`
	
	Example 3: enable the DLDP function for the across-network-segment device 20.1.1.1 with the nexthop ip 10.1.1.1:
	`DES-7200(config)# dldp 20.1.1.1 10.1.1.1`
	
	Example 4: set the resume as 3:
	`DES-7200(config)# dldp 1.1.1.1 resume 3`

4.1.2 dldp passive

Use this command to set the DLDP detection in the passive mode. Use the **no** form of this command to return to the default active DLDP detection mode.

dldp passive

no dldp passive

Parameter description

Parameter	Description
-	-

Default configuration	By default, the DLDP detection is in the active mode.

Command mode	Interface configuration mode.
Usage guidelines	For the point-to-multi-point model, the dldp can be used to set the centralized point as the passive mode to reduce its burden.
Examples	The following example shows how to set the DLDP detection in the passive mode: `DES-7200(config-if)# dldp passive`

4.2 Showing Related Command

4.2.1 show dldp

Use this command to show the UP and DOWN times on the Ethernet interface in a period time.

show dldp interface [**fastEthernet/GigabitEthernet** *interface-number*]

Parameter description

Parameter	Description
interface-number	Specify the Ethernet interface number to the dldp status of next interface only.
Enter	Press the Enter to show the dldp status on all interfaces.

Command mode	Privileged mode.
Usage guidelines	Use this command to show the UP and DOWN times in a period time on one/all Ethernet interfaces. Dldp menas the dldp link configured. Down times: times of the dldp link chaning from UP to DOWN since last reset. Up times: times of the dldp link changing from DOWN to UP since last reset. Start times means the last reset system time

Examples

Example 1: show the dldp state of the Ethernet interface 0/1

```
DES-7200(config)#show dldp fastEthernet  0/0.1
================= FastEthernet 0/0.1 ==================
dldp            down times   up times start time
dldp 8.8.8.1     1            2        1970-0-1 0:0:31
dldp 8.8.8.10    1            2        1970-0-1 0:0:31
dldp 8.8.8.9     1            2        1970-0-1 0:0:31
```

Example 2: show the dldp state of all Ethernet interfaces :

```
DES-7200(config)#show dldp interface
DES-7200#sh dldp interface
==================FastEthernet 0/0 ====================
dldp            down times    up times start time
dldp 7.7.7.1    3             4         2009-1-1 0:0:31
==================FastEthernet0/0.1 ==================
dldp             down times    up times start time
dldp 8.8.8.1      1             1        2009-1-1 0:0:31
dldp 8.8.8.10     1             1        2009-1-1 0:0:31
dldp 8.8.8.9      1             1        2009-1-1 0:0:31
==================FastEthernet 0/1 ====================
dldp             down times   up times start time
dldp 9.7.7.1      3             2        2009-1-1 0:0:31
```

4.3 Clearing Related Command

4.3.1 clear dldp

Use this command to clear the UP and DOWN times recorded by the link DLDP enabled and then recalculates.

clear-dldp {all | destip [*nexthopip*] }

Parameter description

Parameter	Description
destip	Destination IP address for the DLDP detection, which is used to clear the UP and DOWN times recorded in the link with IP address specified.
all	Clear all UP and DOWN times recorded of all Ethernet interfaces.

	destip nexthopip	Clear the UP and DOWN times recorded if the nexthop exists.

Command mode

Privileged mode.

Usage guidelines

The dldp records the number of UP and DOWN. With this command executed, the UP and DOWN times recorded in the specified/all link on the Ethernet interface are cleared and reset to 0.

Examples

Example 1: clear the up/down statistical times of all dldps on the Ethernet interface 0/0:

```
DES-7200(config)#interface fastEthernet 0/0
DES-7200(config-if-FastEthernet 0/0)#clear-dldp all
```

Example 2: clear the up/down statistical times of the dldp 1.1.1.1 on Ethernet interface 0/0:

```
DES-7200(config)#interface fastEthernet 0/0
DES-7200(config-if-FastEthernet 0/0)#clear-dldp 1.1.1.1
```

Example 3: clear the up/down statistical times of the dldp 20.1.1.1 10.1.1.1 on Ethernet interface 0/0:

```
DES-7200(config)#interface fastEthernet 0/0
DES-7200(config-if-FastEthernet 0/0)#clear-dldp
20.1.1.1 10.1.1.1
```

5 RERP Configuration Commands

5.1 Related Configuration Commands

5.1.1 rerp enable

Use this command to enable RERP globally. Use the **no** form of this command to disable the function.

rerp enable

no rerp enable

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Only when the global RERP is enabled, the configuration of other parameters will take effect.
Examples	The following example shows how to enable RERP: `DES-7200(config)# rerp enable`

Related commands

Command	Description
rerp region	Create an RERP domain.

5.1.2 rerp hello-interval

Use this command to configure the interval at which the RERP sends the Hello message on the primary port. Use the **no** form of this command to restore it to the default value.

rerp hello-interval *interval*

no rerp hello-interval

Parameter description

Parameter	Description
interval	Interval of sending the Hello message, in the range 1 to 6 seconds

Default 1 seconds.

Command mode Global configuration mode.

Usage guidelines The detection interval must be less than the failure time.

Examples The following example shows how to set the interval as 2s:

```
DES-7200(config)# rerp hello-interval 2
```

Related commands

Command	Description
rerp fail-interval	Configure the timeout time.

5.1.3 rerp fail-interval

Use this command to configure the maximum time for the RERP to wait on the secondary port to receive the Hello message from the primary port. This time is also used for the backup and transit device to wait before receiving the master IP address and clear packets. Use the **no** form of this command to restore it to the default value.

rerp fail-interval *num*

no rerp fail-interval

Parameter description

Parameter	Description
num	Maximum waiting time in the range 3 to 18 seconds

Default 3 seconds.

Command mode	Global configuration mode.
Usage guidelines	This command is used together with the detection interval and must be larger than the detection interval.
Examples	The following example shows how to set the failure interval as 6 seconds: `DES-7200(config)# rerp fail-interval 6`

Related commands

Command	Description
rerp hello-interval	Configure detection interval.

5.1.4 rerp region

Use this command to create an RERP region and enter the RERP region configuration mode. Use the **no** form of this command to restore it to the default value.

rerp region *num*

no rerp region *num*

Parameter description

Parameter	Description
num	Region ID in the range 1 to 64

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	When a region is created, this device is allowed to enter this region.
Examples	The example below demonstrates how to use this command: `DES-7200# rerp region 1`

Related

Command	Description

commands	**rerp enable**	Enable RERP globally.

5.1.5 ring

Use this command to configure the role, control vlan and primary/secondary port of device in the specified region.

ring *num* **role** [**master** | **backup** | **transit**] **ctrl-vlan** *vid* **primary-port interface** *interface-id* **secondary-port interface** *interface-id*

no ring *num*

Parameter description

Parameter	Description
num	Ring ID.
master|backup|transit	Configure the device as a master/backup/slave device.
vid	Control vlan ID.
interface-id	Interface identifier.

Default N/A.

Command mode RERP region configuration mode.

Usage guidelines Each device plays only one role in a RERP ring. One RERP ring can configure only one master device and one backup device. The port joined the RERP ring is configured as the trunk port automatically, and native vlan is configured as the control vlan automatically.

Examples

```
DES-7200(config)# rerp region 1
DES-7200(config-rerp)# ring 1 role master ctrl-vlan 100
primary-port interface GigabitEthernet 0/1
secondary-port interface GigabitEthernet 0/2
```

Related commands

Command	Description
rerp region	Create an RERP region.

5.1.6 edge-ring

Use this command to configure the sub-ring. One RERP ring shall be configured before this command execution.

edge-ring *num* **role** [**primary-edge|secondary-edge**] **ctrl-vlan** *vid* **shared-port interface** *interface-id* **sub-port interface** *interface-id*

no ring *num*

Parameter description

Parameter	Description
num	Ring ID.
primary-edge|secondary-edge	The device on the primary/secondary edge.
vid	Control VLAN ID.
interface-id	Interface identifier.

Default N/A.

Command mode RERP region configuration mode.

Usage guidelines The shared port must have been configured in a RERP ring before. That is to say, one RERP ring shall be configured before this command execution.

Examples

```
DES-7200(config)# rerp region 1
DES-7200(config-rerp)# edge-ring 2 role primary-edge ctrl-vlan 200 shared-port interface GigabitEthernet 0/1 sub-port interface GigabitEthernet 0/3
```

Related commands

Command	Description
rerp region	Create an RERP domain.
ring	Configure an RERP ring.

5.1.7 major-ring

Use this command to configure the edge-ring for the specified major-ring in order to enable the messages in the edge-ring to be transmitted on the major-ring interface.

major-ring *num* **edge-ring-vlan** *vid*

Parameter description

Parameter	Description
num	Major-ring ID.
vid	Control VLAN ID.

Default N/A.

Command mode RERP region configuration mode.

Usage guidelines Major-ring must have been configured before this command execution.

Examples The example below demonstrates how to use this command:

```
DES-7200(config)# rerp region 1
DES-7200(config-rerp)# major-ring 1 edge-ring-vlan 100
```

Related commands

Command	Description
rerp eanble	Enable RERP globally.
ring	Configure the RERP ring.

5.2 Showing and Monitoring Commands

5.2.1 show rerp

Use this command to show the RERP parameter and status.

show rerp

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show rerp
rerp state                : enable
rerp admin hello interval : 1(*1s)
rerp admin fail interval  : 3(*1s)
rerp edge interval        : 1(*300 ms)
```

```
rerp local bridge         : 001a.a902.fe0b
-----------------------------------
region 1
ring                      : 1
rerp oper hello interval  : 1
rerp oper fail  interval  : 3
ring master                   : 001a.a902.fe0b
ctrl-vlan                     : 100
edge-vlan                     :
role                      : master
primary-port                  : Gi 0/4(forwarding)
secondary-port                : Gi 0/21(down)
```

5.2.2 show rerp statistics

Use this command to show the RERP message statistics.

show rerp statistics region *num* **ring** *ring_id*

Command mode	Privileged EXEC mode.

Examples

```
DES-7200# sh rerp statistics regiong 1 ring 1
The statistics for region 1 ring 1 GigabitEthernet 0/4
TX hello packets       23, RX hello packets         0
TX edge-hello packets   0, RX edge-hello packets
0
TX flush packets        0, RX flush packets         0
TX down packets        0, RX down packets          0
TX up packets             0, RX up packets            0
TX major fail packets   0, RX major fail packets
0
TX major resume packets    0, RX major resume packets  0
TX sub complete packets    0, RX sub complete packets  0

The statistics for region 1 ring 1 GigabitEthernet 0/5
TX hello packets       23, RX hello packets         0
TX edge-hello packets   0, RX edge-hello packets
0
TX flush packets        0, RX flush packets         0
```

```
TX down packets       0, RX down packets          0
TX up packets             0, RX up packets            0
TX major fail packets   0, RX major fail packets
0
TX major resume packets   0, RX major resume packets  0
TX sub complete packets   0, RX sub complete packets  0
```

5.2.3 clear rerp statistics

Use this command to clear the RERP message statistics.

clear rerp statistics

Command mode	Privileged EXEC mode.

5.2.4 debug rerp

Use this command to turn on the RERP service debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug rerp [**packet** | **event**]

undebug rerp [**packet** | **event**]

Parameter description

Parameter	Description
packet	Turn on the incoming/outgoing packet debugging switch.
event	Turn on the event debugging switch.

Command mode	Privileged EXEC mode.

6 REUP Configuration Commands

6.1 Related Configuration Commands

The REUP configuration commands include global configuration commands and interface mode configuration commands.

6.1.1 link state track

Use this command to enable the link state track group. The **no** form of this command is used to disable a link state track group

link state track [*num*]

no link state track [*num*]

Parameter description

Parameter	Description
num	Interface ID of the link aggregation group.

Default N/A.

Command mode Global configuration mode.

Usage guidelines First create a link state track group and then add a port into the specified link state track group.

Examples The following example shows how to create a link state track group:

```
DES-7200(config)# link state track 1
```

Related commands

Command	Description
link state group	Add the port to the specified link state track group.

6.1.2 link state group

Use this command to add the port into the specified link state track group. The **no** form of this command is used to delete a port from the specified link state track group.

link state group *num* {**upstream | downstream**}

no link state group

Parameter description

Parameter	Description
num	ID of the link state track group.
upstream	Configure the port to be an upstream port in the link state track group.
downstream	Configures the port to be a downstream port in the link state track group.

Default

The port is not added into any link state track group.

Command mode

Interface configuration mode.

Usage guidelines

First create a link state track group and then add a port into the specified link state track group.

Examples

The following example shows how to add the port fa0/2 into the link state track group:

```
DES-7200(config)# link state track 1
DES-7200(config)# interface fa 0/2
DES-7200(config-if)# link state group 1 upstream
```

Related commands

Command	Description
link state track	Enable a link state track group.

6.1.3 mac-address-table move update max-update-rate

Use this command to configure the maximum number of MAC address update packets sent per second.

mac-address-table move update max-update-rate *pkts-per-second*

no mac-address-table move update max-update-rate

Parameter description

Parameter	Description
pkts-per-second	The maximum number of MAC address update packets sent per second. It ranges from 0 to 32000, and the default value is 150.

Default

A maximum of 150 MAC address update packets are sent per second.

Command mode

Global configuration mode.

Usage guidelines

When a link is switched, REUP sends a certain number of MAC address update packets to an uplink device in every second to recover downlink data transmission of the uplink device.

Examples

The following example shows how to configure the maximum number of MAC address update packets sent per second:

```
DES-7200(config)# mac-address-table move update
max-update-rate 20
```

Related commands

Command	Description
-	-

6.1.4 switchport backup interface *interface-id*

Use this command to configure the REUP dual link backup interface.

switchport backup interface *interface-id*

no switchport backup

Parameter description

Parameter	Description
Interface-id	Interface ID of the backup link.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines Enter the primary interface configuration mode, the interface-id in the parameter is for the backup interface. When the active link fails, the backup link transmission is restored rapidly.

Examples The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as primary interface and backup interface:

```
DES-7200(config)# interface fa 0/1

DES-7200(config-if)# switchport backup interface fa 0/2
```

Related commands

Command	Description
show interface switchport backup	View the dual link backup configuration on the switch.

6.1.5 switchport backup interface *interface-id* preemption

Use this command to configure the REUP link preemption function.

switchport backup interface *interface-id* **preemption mode** {**forced** | **bandwidth** | **off** }

switchport backup interface *interface-id* **preemption delay** *delay-time*

no switchport backup interface *interface-id* **preemption delay**

Parameter description

Parameter	Description
interface-id	The interface id of the backup link.
delay-time	The preemption delay time.

Default	The preemption function is disabled by default. The default preemption delay time is 35s.
Command mode	Interface configuration mode.
Usage guidelines	The preemption mode includes **forced, bandwidth and off**. In the **bandwidth** preemption mode, the interface with high bandwidth has priority over other interfaces to transmit the data. In the **forced** preemption mode, the primary has priority over backup interfaces to transmit the data. No preemption event occurrs in the **off** preemption mode. By default, the preemption mode is off. The preemption delay refers to the delay time of the link reswitch after the restoration of the link failure.

Examples	The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as the primary interface and backup interface, set the bandwidth preemption mode and 40s preemption delay:
	`DES-7200(config)# interface fa 0/1`
	`DES-7200(config-if)# switchport backup interface fa 0/2`
	`preemption mode bandwitdh`
	`DES-7200(config-if)# switchport backup interface fa 0/2`
	`preemption delay 40`

Related commands

Command	Description
show interface switchport backup	View the dual link backup configuration.

6.1.6 mac-aadress-table move update receive

Use this command to enable REUP to receive the mac-address-table update messages.

mac-address-table move update receive

no mac-address-table move update receive

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The dual link backup switchover will lead to the loss of downstream data flow, for the MAC address for the uplink switch has not been updated in time. Therefore, it is necessary to update the MAC address table of the uplink switch, to reduce the loss of L2 data flow. You need to enable the switch of receiving the MAC address update messages on the uplink switch.
Examples	`DES-7200(config)# mac-address-table move update receive`

Related commands

Command	Description
mac-address-table move update transit	Enable REUP to transmit the mac-address-table update messages.

6.1.7 mac-aadress-table move update receive vlan

Use this command to configure the VLANs processing MAC address update packets.

mac-address-table move update receive vlan *vlan-range*

no mac-address-table move update receive vlan *vlan-range*

Parameter description

Parameter	Description
vlan-range	Range of the VLANs processing MAC address update packets.

Default	All VLANs process MAC address update packets.
Command mode	Global configuration mode.
Usage guidelines	This command can be used to disable some VLANs from processing MAC address update packets. VLANs disabled

from processing MAC address update packets can still recover downlink data transmission of the uplink device using MAC address update packets, but the capability to provide convergence on link failure will be degraded.

Examples

The following example configures VLANs processing MAC address update packets:

```
DES-7200(config)# no mac-address-table move update receive vlan 20
```

Related commands

Command	Description
mac-address-table move update receive	Enable REUP to receive MAC address update packets.

6.1.8 mac-address-table move update transit

Use this command to enable REUP to transmit the mac-address-table update messages.

mac-address-table move update transit

no mac-address-table move update transit

Default Disabled.

Command mode Global configuration mode.

Usage guidelines

In order to reduce the link switchover and the loss of the downstream data flow, it is necessary to enable the switch of receiving the MAC address update messages on the uplink switch.

Examples

```
DES-7200(config)# mac-address-table move update transit
```

Related commands

Command	Description
mac-address-table move update transit vlan	Enable REUP to transmit the mac-address-table update messages.

6.1.9 mac-address-table move update transit vlan

Use this command to enable REUP to transmit the mac-address update messages.

mac-address-table move update transit vlan *vid*

no mac-address-table move update transit vlan

Parameter description

Parameter	Description
vid	ID of the VLAN transmitting MAC address update packets.

Default

Transmit the MAC-address update messages in the default VLAN on the port.

Command mode

Interface configuration mode.

Usage guidelines

When a link is switched, the VLAN enabled to transmit MAC address update packets will send MAC address update packets to its uplink device.

Examples

The following example configures VLANs transmitting MAC address update packets:

```
DES-7200(config)# mac-address-table move update transit
```

Related commands

Command	Description
mac-address-table move update transit	Enable REUP to receive the mac-address-table update messages.

6.1.10 mac-address-table update group

Use this command to set the mac-address-table update group.

mac-address-table update group [*group-num*]

no mac-address-table update group

Parameter description

Parameter	Description
group-num	The mac-address-table update group

	ID.

Default

The default group number is 1.

By default, no mac-address-table update group is configured.

Command mode

Interface configuration mode.

Usage guidelines

In order to reduce the flood due to the MAC address update and the influence on the normal data transmission of the switch, DES-7200products add a configuration of MAC address update group. Only if all the interfaces are added to a MAC address update group, the downstream data transmission be restored rapidly.

Examples

```
DES-7200(config-if)# mac-address-table update group 2
```

Related commands

Command	Description
show mac-address-table update group detail	Show the mac-address-table update group information.

6.1.11 switchport backup interface *interface-id* prefer instance

Use this command to configure VLAN load balancing on a link. The **no** form of this command is used to delete the configured VLAN load strategy.

switchport backup interface *interface-id* **prefer instance** *instance-range*

no switchport backup interface *interface-id* **prefer**

Parameter description

Parameter	Description
interface-id	Interface ID of the backup link.
instance-range	Instance range of loading on the backup interface.

Default

No VLAN load on the backup interface.

Command mode

Interface configuration mode.

Usage guidelines

MSTP instance mapping can be used to modify the mapping between an instance and a VLAN.

Examples

The following example configures VLAN load balancing on dual links.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport backup interface gigabitEthernet 0/2 prefer instance 1
```

Related commands

Command	Description
show interface switchport backup	Show the configuration of dual-link backup on the switch.
spanning-tree mst configuration	Configure MSTP instances.

6.2 Showing and Monitoring Commands

6.2.1 show link state group

Use this command to show the information of a link state track group.

show link state group *num*

Parameter description

Parameter	Description
num	ID of a link state track group.

Default

None

Command mode

Privileged EXEC mode.

Examples

The following example shows the link state track group:

```
DES-7200# show link state group
Link State Group:1  Status: Enabled, UP
Upstream Interfaces :Gi0/1(Up)
Downstream Interfaces :Gi0/3(Dwn), Gi0/4(Dwn)
```

```
Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :
(Up):Interface up (Dwn):Interface Down (Dis):Interface
disabled
```

6.2.2 show interfaces [*interface-id*] switchport backup [detail]

Use this command to show the dual link backup information on the interfaces.

show interfaces [*interface-id*] **switchport backup** [**detail**]

Parameter description

Parameter	Description
interface-id	The interface id of the dual link backup.
detail	Show the detailed information about the dual link backup.

Default Show the dual link backup information on all interfaces.

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface     Backup Interface      State
------------------------------------------------
Gi0/23                  Gi0/24                   Active
Up/Backup Standby
Interface Pair : Gi0/23, Gi0/24
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi0/23(1000 Mbits), Gi0/24(1000 Mbits)
```

6.2.3 show mac-address-table update group detail

Use this command to show the mac-address-table update group information.

show mac-address-table update group detail

Parameter description

Parameter	Description
detail	Show the detailed information about the mac-address-table update group.

Default

Show the mac-address-table update group information.

Command mode

Privileged EXEC mode.

Examples

```
DES-7200# configure terminal
DES-7200(config)# mac-address-table move update receive
DES-7200(config)# interface range gigabitEthernet 0/3-4
DES-7200(config-if-range)#  mac-address-table  update
group
DES-7200(config-if-range)# end
DES-7200# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:7
Group member  Receive Count  Last Receive Switch-ID
Receive Time
------------------------------------------------------
-----
GigabitEthernet 0/3  0             0000.0000.0000

GigabitEthernet 0/4  0             0000.0000.0000
```

7 RLDP Configuration Command

7.1 Configuration Related Commands

The RLDP configuration commands include global configuration commands, interface mode configuration commands and privilege mode configuration commands.

7.1.1 rldp enable

Use this command to enable RLDP globally. Use the **no** form of this command to disable the function.

rldp enable

no rldp enable

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	You can enable RLDP on the interface only when the global RLDP is enabled.
Examples	The following example shows how to enable RLDP: `DES-7200(config)# rldp enable`

Related commands

Command	Description
rldp port	Enable the RLDP function on the port.

7.1.2 rldp detect-interval

Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the **no** form of this command to restore it to the default value.

rldp detect-interval *interval*

no rldp detect-interval

Parameter description

Parameter	Description
interval	Detection interval in the range 2 to 15 seconds

Default 3 seconds.

Command mode Global configuration mode.

Usage guidelines In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.

Examples The following example shows how to set the detection interval as 5s:

```
DES-7200(config)# rldp detect-interval 5
```

Related commands

Command	Description
rldp detect-max	Set the maximum number of detections.

7.1.3 rldp detect-max

Use this command to set the maximum number of sending detection packets on the port. If the neighboring port does not respond when this detection number is exceeded, the link is considered faulty. Use the **no** form of this command to restore it to the default value.

rldp detect-max *num*

no rldp detect-max

Parameter description

Parameter	Description
num	Maximum number of detections in the range 2 to 10

Default 2.

Command mode Global configuration mode.

Usage guidelines This command is used together with the detection interval to specify the maximum number of detections.

Examples The following example shows how to set the maximum number of detections as 5:

```
DES-7200(config)# rldp detect-max 5
```

Related commands

Command	Description
rldp detect-interval	Set the detection interval.

7.1.4 rldp port

Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the **no** form of this command to disable the function.

rldp port {**unidirection-detect | bidirection-detect | loop-detect** } **{warning | shutdown-svi | shutdown-port | block}**

no rldp port { **unidirection-detect | bidirection-detect | loop-detect** }

Parameter description

Parameter	Description
unidirection-detect	Set unidirectional link detection.
bidirection-detect	Set bidirectional link detection.
loop-detect	Set loop detection type.
warning	Warn the user.
shutdown-svi	Shutdown the SVI the port belongs to.

shutdown-port	Shutdown the port.
block	Disable the learning-forwarding function of the port.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines The RLDP detection on the port takes effect only when the global RLDP is enabled.

Examples The following example demonstrates how to configure RLDP detection on fas 0/1, specify the detection type as loop detection, and troubleshooting method as block.

```
DES-7200(config)# interface fas 0/1
DES-7200(config-if)# rldp port loop-detect block
```

Related commands

Command	Description
rldp enable	Enable RLDP globally.

7.1.5 rldp reset

Use this command to make all the ports that have been handled using **rldp shutdown** or **disable** to perform RLDP detection again.

rldp reset

Parameter description N/A.

Default N/A.

Command mode Privileged EXEC mode.

Examples The example below demonstrates how to use this command:

```
DES-7200# rldp reset
```

Related commands	Command	Description
	rldp eanble	Enable RIDP globally.

7.2 Showing and Monitoring Commands

7.2.1 show rldp

Use this command to show the RLDP information.

show rldp [**interface** *interface-id*]

Parameter description	Parameter	Description
	interface-id	Interface ID

Command mode	
	Privileged EXEC mode.

7.2.2 debug rldp

Use this command to turn on the RLDP service debugging switch. The **no** form of this command is used to turn off the debugging switch.

- **debug rldp** [**packet | event | error**]
- **undebug rldp** [**packet | event | error**]

Parameter description	Parameter	Description
	packet	Turn on the incoming/outgoing RLDP packet debugging switch.
	event	Turn on the event debugging switch.
	error	Turn on the error debugging switch.

Command mode	
	Privileged EXEC mode.

8 TPP Configuration Commands

8.1 Configuration Related Commands

8.1.1 topology guard

In the global configuration command mode, use this command to enable the topology protection function. Use the **no** form of this command to disable the topology protection function.

[no] topology guard

Default configuration	Enabled.
Command mode	Global configuration mode.
Usage guidelines	The topology protection function is enabled by default, so as to protect the network against topology oscillation due to attacks. It should be used with the **cpu topology-limit** command.

Examples	The following example shows how to enable and disable the global topology protection function:
	`DES-7200(config)# topology guard`
	`DES-7200(config)# no topology guard`

Related commands

Command	Description
tp-guard port enable	Enable the topology protection function on the interface.
cpu topology-limit	Set the CPU utilization limitation.

8.1.2 tp-guard port enable

Use this command to enable the topology protection function on the port. Use the **no** form of this command to disable the function.

[**no**] **tp-guard port enable**

Parameter description	N/A.
Default configuration	N/A.
Command mode	Interface configuration mode.
Usage guidelines	If both the global topology protection function and the topology protection function of the port are enabled, the remote device of this port will be notified when the CPU utilization of the local device is too high or there are other problems with the local device. This command is applicable to the layer 2 switching interfaces and routing interfaces. Other interfaces (including AP member port) do not support this command.

Examples	The following example shows how to configure the topology protection function for the port:
	`DES-7200(config-if)# tp-guard port enable`
	`DES-7200(config-if)# no tp-guard port enable`

Related commands

Command	Description
topology guard	Enable the topology protection function globally.

8.2 Showing Related Commands

8.2.1 show tpp

Use this command to show the configuration of topology protection.

show tpp

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the current TPP configuration and port detection.
Examples	The following example shows how to display information about the topology protection function: `DES-7200# show tpp`

Related commands

Command	Description
topology guard	Enable the topology protection function globally.

9 NLB GROUP Configuration Commands

9.1 Configuration Related Commands

9.1.1 nlb-group

Use this command to create a cluster group and specify the cluster's attributes (VRF, IP address and reflector port) or the port connecting the cluster with device. The **no** form of this command is used to delete the cluster's attributes or delete the port connecting with the cluster separately.

nlb-group *group-number* [**vrf** *vrf-name*] **ip** *nlb-address* [**reflector-port** *interface-name*]

nlb-group *group-number* **destination-port** *interface-name*

no nlb-group *group-number* [[**vrf** *vrf-name*] **ip** *nlb-address* [**reflector-port** *interface-name*]]

no nlb-group *group-number* [**destination-port** *interface-name*]

no nlb-group all

Parameter description

Parameter	Description
group-number	Cluster group number
vrf-name	VRF name
nlb-address	NLB address
reflector-port *interface-name*	Reflector port, which serves as a relay port to send the packets to the cluster. For the interface-name, please specify the corresponding interface number and it can be the physical port (the L2AP excluded) only.

	destination-port *interface-name*	Port connecting the cluster with device. For the interface-name, please specify the corresponding interface number and it can be the physical port (the L2AP included) only, but not the SVI or Routed Port.

Default configuration	N/A

Command mode	Global configuration mode.

The Switch Port and L2AP can be both configured as the cluster connecting port. However, only the Switch Port can be set as the reflector port. Only after configuring the cluster's VRF, IP address and reflector port, the packets are allowed to be routed to the connecting port. If no cluster's connecting port is configured, the packets will flood in the VLAN belonging to the cluster.

With the cluster's VRF, IP address and reflector port deleted, the packets routed to the cluster can only be routed to the single server of the cluster.

When deleting, if no cluster attributes or connecting ports are specified, the entire cluster group will be removed.

Use the command **show nlb-group** to show the cluster configurations.

Usage guidelines

Caution

- After a port has been configured as a reflector port, other configurations are not allowed for this port.
- One port can not be both the reflector port and connecting port.
- After configuring the cluster attributes, the cluster service is enabled only on the connecting port with cluster configured.
- If no cluster attribute is configured, the cluster service is not enabled.
- No VRF keyword means the global VRF takes effect.
- Up to 5 cluster groups can be configured on each switch and up to16 connecting ports are configurable on per cluster group.

Examples

The following example creates a cluster group and configures the cluster attributes and the cluster connecting port.

```
DES-7200(config)# nlb-group 1 vrf vpn-1 ip 192.168.10.1 reflector-port gigabitethernet 0/1
DES-7200(config)# nlb-group 1 destination-port gigabitethernet 0/2, 0/3
```

The following example deletes the cluster attributes of cluster group1:

```
DES-7200(config)# no nlb-group 1 vrf vpn-1 ip 192.168.10.1 reflector-port gigabitethernet 0/1
```

The following example deletes the connecting port of cluster group1.

```
DES-7200(config)# no nlb-group 1 destination-port gigabitethernet 0/2, 0/3
```

Related commands

Command	Description
show nlb-group	Show the cluster configurations.

Platform description -

9.2 Show Related Command

9.2.1 show nlb-group

Use this command to show the cluster configuations.

show nlb-group [*group_number*].

Parameter description

Parameter	Description
group-number	Cluster group number

Default configuration All cluster groups are shown by default.

Command mode Privileged mode.

Usage guidelines N/A

Examples

The following example shows the cluster configurations.

```
DES-7200# show nlb-group 1
group-number： 1
cluster-vrf: vpn-1
cluster-ip: 192.168.10.1
destination-port: Gi 0/2, Gi 0/3, Gi 0/3
```

Field	Description
group-number	Cluster group number.
destination-port	Port connecting the cluster with device.
cluster-vrf	Cluster VRF name.
cluster-ip	Cluster IP address.
reflector-port	Reflector port.

Related commands

Command	Description
nlb-group	Create a cluster group and specify the cluster attributes and the port connecting the cluster with device.

Command mode

-

10 Supervisor Engine Redundancy Configuration Commands

10.1 Related Configuration Commands

The configuration commands for supervisor engine redundancy include the redundant mode commands and privileged mode commands.

10.1.1 auto-sync

Use this command to synchronize runing-config and startup-config in the case of redundancy of dual supervisor engines. Use the **no** form of this command to disable the function.

auto-sync { **standard | running-config | startup-config}**

no auto-sync { **standard | running-config** | **startup-config**}

Parameter description

Parameter	Description
standard	Synchronize all the system files.
running-config	Synchronize the runtime configuration files.
startup-config	Synchronize the startup configuration files.

Default All the files are synchronized by default.

Command mode Redundancy configuration mode.

Usage guidelines Generally the **standard** synchronization should be used if there is no special requirement.

Examples

The following example only synchronizes the **startup-config** files

```
DES-7200(config)# redundancy
DES-7200(config-red)# auto-sync startup-config
DES-7200(config-red)# exit
```

The following example synchronizes all the files other than the starup-config files.

```
DES-7200(config)# redundancy
DES-7200(config-red)# no auto-sync startup-config
DES-7200(config-red)# exit
```

Platform description

This command is supported on DES-7200.

10.1.2 auto-sync time-period

Use this command to configure the auto-sync time-period of runing-config and startup-config when the dual supervisor engines is redundant. Use the **no** form of this command to disable the function.

auto-sync time-period *value*

no auto-sync time-period

Parameter description

Parameter	Description
value	Auto-sync time-period interval (second).

Default

Auto-sync with 1 hour (3600 seconds) time-period interval

Command mode

Redundancy configuration mode.

Usage guidelines

Use standard synchronization if there is no particular demand.

Examples	The following example only synchronizes the startup-config file:
	`DES-7200(config)# redundancy`
	`DES-7200(config-red)# auto-sync time-period 60`
	`Redundancy auto-sync time-period: enabled (60 seconds).`
	`DES-7200(config-red)# exit`
	The following example disables auto-sync:
	`DES-7200(config)# redundancy`
	`DES-7200(config-red)# no auto-sync time-period`
	`Redundancy auto-sync time-period: disabled.`
	`DES-7200(config-red)# exit`

Platform description	This command is supported on DES-7200.

10.1.3 redundancy

Use this command to enter redundancy configuration mode in the global configuration mode.

redundancy

Command mode	Global configuration mode.
Usage guidelines	Enter the redundancy configuration mode in the global configuration mode to execute the redundant mode commmands like auto-sync、auto-sync time-period、switchover timeout,etc, to do the related redundancy configuration.

Examples	`DES-7200# config terminal`
	`DES-7200(config)# redundancy`
	`DES-7200(config-red)# exit`

Platform description	This command is supported on DES-7200.

10.1.4 redundancy reload

In the privileged EXEC mode, use the **redundancy reload** command to reset slave device or reset both master and slave devices.

redundancy reload {**peer** | **shelf**}

Parameter description

Parameter	Description
peer	Reset the slave device only.
shelf	Reset the master and slave devices.

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	The **redundancy reload peer** does not affect the data transfer. During the resetting of the Slave, the data transfer is not disconnected and the user session information is not lost.

Examples

```
DES-7200# redundancy reload peer
Reload peer? [confirm] y
Preparing to reload peer
```

Related commands

Command	Description
reload	Reset the master supervisor engine.

Platform description	This command is supported on DES-7200.

10.1.5 redundancy forceswitch

In privileged EXEC mode, use this command to enforce Slave supervisor engine to switchover.

redundancy forceswitch

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command allows you to select the slot in which the supervisor engine serves as the master supervisor engine and that as the slave supervisor engine, or the slot in which the supervisor engine is superior to that in another slot as the master board.
Examples	`DES-7200# redundancy forceswitch` `Proceed with switchover to standby PRE? [confirm]y`

Related commands

Command	Description
reload	Reset the master supervisor engine.

Platform description	This command is supported on DES-7200.

10.1.6 switchover timeout

In the redundancy configuration mode, use the **switchover timeout** command to configure the switchover timeout value for the supervisor engine. Use the **no** form of this command to restore the timeout to the default value.

switchover timeout *timeout-period*

no switchover timeout

Parameter description

Parameter	Description
timeout-period	Switchover timeout in the range 160 to 25,000 (milliseconds).

Default	4000 milliseconds.

Command mode	Redundancy configuration mode.
Usage guidelines	When the slave device has not received a heartbeat message of the master device within the timeout period, the switchover will occur. If you are not sure, do no modify the default value.
Examples	DES-7200# **config terminal** DES-7200(config)# **redundancy** DES-7200(config-red)# DES-7200(config-red)# **switchover timeout 4000** DES-7200(config-red)# **exit** DES-7200(config)# **exit** DES-7200(config)#
Platform description	This command is supported on DES-7200.

10.2 Showing and Monitoring Commands

10.2.1 show redundancy auto-sync

Use command **show redundancy auto-sync** to show the current redundancy auto-sync mode in user EXEC or privileged EXEC mode. For the detailed information, please refer to auto-sync description in previous text.

show redundancy auto-sync

Default	N/A
Command mode	User mode or Privileged EXEC mode.
Examples	DES-7200> **enable** DES-7200# **show redundancy auto-sync** Redundancy auto-sync mode: auto-sync standard. ...

Platform description	This command is supported on DES-7200.

10.2.2 show redundancy states

Use this command to show the current redundancy in the user mode or privileged EXEC mode.

show redundancy states

Parameter description

Parameter	Description
states	Show the redundancy status of the master or the slave devices.

Default	N/A.
Command mode	User mode or privileged EXEC mode
Usage guidelines	N/A.

Examples

```
DES-7200> enable
DES-7200# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
DES-7200# show redundancy states
Redundancy states:
         My state = 19 -ACTIVE
       peer state = 37 -STANDBY HOT
...
```

Platform description	This command is supported on DES-7200.

10.2.3 show redundancy switchtimeout

Use **show redundancy switchtimeout** command to show current redundanct switchover timeout time in user EXEC or privileged EXEC mode.

show redundancy switchtimeout

Default	N/A
Command mode	User mode or Privileged EXEC mode.
Examples	DES-7200> **enable** DES-7200# **show redundancy switchtimeout** redundancy switch timeout is : 4000 ms. ...
Platform description	This command is supported on DES-7200.

DES-7200
System Management Command Reference Guide
Version 10.4(3)

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)
Date:

Copyright Statement

D-Link Corporation ©2011
All rights reserved.
Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

Caution Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 File System Configuration Commands

1.1 Configuration Related Commands

1.1.1 cd

Use this command to set the present directory for the filesystem.

cd [*filesystem:*][*directory*]

Parameter description

Parameter	Description
filesystem:	Specified file system. This parameter must be carried with ":".
directory	Specified directory

Default

The default directory is the flash root directory.

Command mode

Privileged EXEC mode.

Usage guidelines

Change the above parameter to the directory you want to enter. Use the **pwd** command to view the present directory.

Examples

The following example sets usb0 root directory as the present directory:

```
DES-7200# cd usb0:/
```

The following example sets sd root directory as the present directory:

```
DES-7200# cd sd0:/
```

Related

Command	Description

commands	**pwd**	Show the present word directory.

1.1.2 copy

Use this command to copy a file from the specified source directory to the specified destination directory.

copy *source-url destination-url*

Parameter description

Parameter	Description
source-url	Source file URL, which can be local or remote.
destination-url	Destination file URL, which can be local or remote.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines

This command is used to copy the files among various storage media in the local and to transmit the files between the network servers:

The following table lists the URL prefix for the specified file system:

Prefix	Description
flash:	Flash storage media. This prefix can be used in all devices. The default is flash if the prefix is not used for the URL. In general, the bootstrap main program is stored in the flash.
tftp:	TFTP network server
xmodem:	Use the xmodem protocol to transmit the file to the network device.
slave:	Flash on the slave board from the chassis device.
usb0:	The first USB device.
usb1:	The second USB device.
sd0:	The first SD card.

sw1-m1-disk0:	Management board on the M1 slot of the chassis with switch id 1, in the VSU mode.
sw1-m2-disk0:	Management board on the M2 slot of the chassis with switch id 1, in the VSU mode.
sw2-m1-disk0:	Management board on the M1 slot of the chassis with switch id 2, in the VSU mode.
sw2-m2-disk0:	Management board on the M2 slot of the chassis with switch id 2, in the VSU mode.

Caution

This command does not support the wildcard.

Note

Without the specified URL prefix configured, it refers to the current file system.

Examples

Example 1: Download the file from the tftp server:

```
DES-7200# copy tftp://192.168.201.54/firmware.bin
flash:/
```

Example 2: Upload the file to the tftp server:

```
DES-7200# copy flash:/firmware.bin
tftp://192.168.201.54/firmware.bin
```

Example 3: Use the xmodem protocol to download the file:

```
DES-7200# copy xmodem: flash:/config.text
```

Example 4: Copy the file to the U disk:

```
DES-7200#copy flash:/config.text usb0:/config.text
```

Example 5: Copy the file to the slave management board:

```
DES-7200#copy flash:/config.text slave:/config.text
```

Example 6: Copy the file from the flash to the SD card:

```
DES-7200#copy flash:/firmware.bin sd0:/firmware.bin
```

Example 7: Copy the file from the U disk to the SD card:

```
DES-7200#copy usb0:/config.text sd0:/config.text
```

Example 8: Copy the file from the SD card to the U disk:

```
DES-7200#copy sd0:/config.text usb0:/config.text
```

Related commands

Command	Description
delete	Delete the file.
rename	Rename the file.
dir	Show the file list of the specified directory.

1.1.3 delete

Use this command to delete the files in the present directory.

delete *url*

Parameter description

Parameter	Description
url	The URL for the file to be deleted.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines

This command is used to delete the specified file in the URL. This command supports deleting the files stores in the local storage media, i.e., the URL must be one of the flash:/ usb0:/ or usb1:/ slave:/. If the prefix is not specified in the URL, it indicates to delete the file in the system.

This command does not support wildcard.

Examples

Example 1: Delete the `tmpfile` from the present directory:

```
DES-7200# delete tmpfile
```

Example 2: Delete the `firmware.bin.bak` from the

secondary board:

```
DES-7200# delete slave:/firmware.bin.bak
```

Example 3: Delete the `aaa.bin` form the SD card:

```
DES-7200# delete sd0:/aaa.bin
```

Related commands

Command	Description
copy	Copy the file.
dir	Show the file list of the specified directory.

1.1.4 dir

Use this command to show the files in the present directory.

dir [*filesystem:*][*directory*]

Parameter description

Parameter	Description
filesystem	Set the filesystem for the file to be displayed. This parameter must carry with ":".
directory	Set the directory for the file to be displayed.

Default

By default, only the information under the present working path is shown.

Command mode

Privileged EXEC mode.

Usage guidelines

Enter the specified directory to show the information of all the files in that directory. If no parameter is specified, the information of the files in the present directory is shown by default.

This command does not support wildcard.

Examples

Example 1: Show the file information of the root directory in the slave board:

```
DES-7200# dir slave0:/
Directory of slave:/
```

```
   Mode Link     Size             MTime Name
--------      ----      ---------      -------------------
------------------
          1  10838016 2008-01-01 00:01:53 firmware.bin
          1      399 2008-01-01 00:01:37 config.text
          1      399 2008-01-01 00:17:58 cfg.txt
------------------------------------------------------------
----
3 Files (Total size 11210782 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20463616 bytes
(19MB) available.
```

Example 2: Show the information of all the files in the present directory:

```
DES-7200# dir
Directory of temp:/
   Mode Link     Size             MTime Name
--------      ----      ---------      -------------------
------------------
          1      399 2008-01-01 00:17:58 a.dat
------------------------------------------------------------
----
1 Files (Total size 399 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20463616 bytes
(19MB) available.
```

Related commands

Command	Description
pwd	Show the present directory.
cd	Set the present directory of the filesystem.

1.1.5 mkdir

Use this command to create a directory.

mkdir directory

Parameter description

Parameter	Description
directory	Name of the directory to be created.

Default N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	Simply enter the name of the directory you want to create (including the path). Note: If the created file has been existed, the creation will fail. If the upper-level for the directory to be created is inexistent, it fails to create the specified directory. For example, if the directory of flash:/backup is inexistent, the creation of the directory of flash:/backup/temp will fail. The solution is that the directory of flash:/backup shall be created before the creation of the directory of flash:/backup/temp.

Examples	Example 1: Create the test directory at the root directory:
	`DES-7200# **mkdir** *test*`
	
	Example 2: Create the test2 directory at the root directory of the SD card:
	`DES-7200# **mkdir** *sd0:/test2*`

Related commands

Command	Description
rmdir	Delete the directory.
pwd	Show the present directory.

1.1.6 rename

Use this command to move or rename the specified file.

rename *url1 url2*

Parameter description

Parameter	Description
url1	The source file URL to move.
url2	The URL of the destination file or directory.

Default	N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command only supports to move the local file, but not to transfer the file to the server using the protocol. The supported prefixes are: usb0/1, flash and slave.

Examples	Example 1: Move the `log.txt` to the upper-level directory and rename it `config.txt`:
	`DES-7200# **rename** *tmp/log.txt ../config.txt*`
	
	Example 2: Move the `log.txt` in the slave board to the usb0 device:
	`DES-7200# **rename** slave:/log.txt usb0:/log.txt`
	
	Example 3: Rename the `log.txt` in the present directory as `log.txt.bak`:
	`DES-7200# **rename** log.txt log.txt.bak`
	
	Example 4: Move the `dnos.bin` in the SD card to the flash:
	`DES-7200# **rename** sd0:/dnos.bin flash:/dnos_bak.bin`
	
	Example 5: Move the `test.txt` in the U disk to the SD card:
	`DES-7200# **rename** usb0:/test.txt sd0:/test2.txt`

Related commands

Command	Description
delete	Delete the file.
copy	Copy the file.

1.1.7 rmdir

Use this command to delete an empty directory.

rmdir directory

Parameter description

Parameter	Description
directory	Name of the directory to be deleted, which must be empty

Default N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command does not support the wildcards, and the directory to be deleted must be empty. Since this command supports abbreviations, you can also use the **rm** command to delete empty directories.

Examples	If there is tmp directory in the present directory and the directory does not contain any files:
	`DES-7200# rmdir tmp`
	`DES-7200# ls`

1.2 Showing Related Commands

1.2.1 pwd

Use this command to show the working path.

pwd

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command shows the present working path

Examples	The following example shows the present working path.
	`DES-7200# pwd`
	`Flash:/`

Related commands

Command	Description
cd	Change the file system in the present directory.

1.2.2 show file systems

Use this command to show the file system information.

show file systems

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to show the file systems supported in the present devices and the available space condition in the file system.
Examples	Show the file system information: `DES-7200# show file systems`

2 Configuration Commands of Configuration File Management

2.1 Configuration Related Command

2.1.1 archive

Use this command to switch to the archive configuration mode. The **no** form of this command can be used to restore all configurations in the archive configuration mode to the default state.

archive

no archive

Parameter description

Parameter	Description
-	-

Default -

Command mode Global configuration mode.

Usage guidelines

Use the **archive** command to switch to the archive configuration mode.

Use the **end** command or enter CTRL+C to return to the privileged mode.

Use the **exit** command to return to the global configuration mode.

Examples

The following example switches to the archive configuration mode:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with
```

CNTL/Z.

DES-7200(config)# **archive**

Related commands	**Command**	**Description**
	-	-

2.1.2 hidekeys

Use this command to prohibit showing the passwords in the configuration log. The **no** form of this command can be used to allow showing the passwords in the configuration log.

hidekeys

no hidekeys

Parameter description	**Parameter**	**Description**
	-	-

Default Allow showing the passwords in the configuration log by default.

Command mode Archive log management configuration mode

Usage guidelines N/A.

Examples The following example prohibits showing the passwords in the configuration log:

DES-7200# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

DES-7200(config)# **archive**

DES-7200(config-archive)# **log config**

DES-7200(config-archive-log-config)# **hidekeys**

Related commands	**Command**	**Description**
	archive	Enter the archive configuration mode.
	log config	Enter the archive log management configuration mode.

	logging enable	Enable the function of logging the configuration change

2.1.3 log config

Use this command to switch to the archive log management configuation mode. The no form of this command is used to restore all configurations in this configuration mode to the default state.

log config

no log config

Parameter description

Parameter	Description
-	-

Default N/A.

Command mode Archive configuration mode

Usage guidelines

Use the **log config** command to switch to the archive log management configuration mode.

Use the **end** command or enter CTRL+C to return to the privileged mode.

Use the **exit** command to return to the archive configuration mode.

Examples

The following example switches to the archive log management configuration mode:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# archive
DES-7200(config-archive)# log config
```

Related commands

Command	Description
archive	Enter the archive configuration mode.

2.1.4 logging enable

Use this command to enable the function of logging the configuration change. The **no** form of this command is used to disable this function.

logging enable
no logging enable

Parameter description

Parameter	Description
-	-

Default Disabled

Command mode Archive log management configuration mode

Usage guidelines N/A

Examples

The following example enables the function of logging the configuration change:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# archive
DES-7200(config-archive)# log config
DES-7200(config-archive-log-config)# logging enable
```

Related commands

Command	Description
archive	Enter the archive configuration mode.
log config	Enter the archive log management configuration mode.

2.1.5 logging size

Use this commad to specify the maximum number of the entries saved in the configuration log. The **no** form of this command is used to restore it to the default value.

logging size *entries*
no logging size

Parameter description

Parameter	Description
entries	The maximum number of the entries saved in the configuration log, in the range of 1 to 1000.

Default 100

Command mode Archive log management configuration mode

Usage guidelines N/A

Examples

The following example specifies the maximum number of the entries saved in the configuration log as 50:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# archive
DES-7200(config-archive)# log config
DES-7200(config-archive-log-config)# logging size 50
```

Related commands

Command	Description
archive	Enter the archive configuration mode.
log config	Enter the archive log management configuration mode.

2.1.6 notify syslog

Use this command to allow sending the configuration change notification to the remote log server. The **no** form of this command can be used to prohibit sending the configuration change notification to the remote log server.

notify syslog

no notify syslog

Parameter description

Parameter	Description
-	-

Default	Prohibit sending the configuration notification to the remote log server by default.
Command mode	Archive log management configuration mode
Usage guidelines	N/A

Examples	The following example allows sending the configuration change notification to the remote log server:
	`DES-7200# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`DES-7200(config)# archive`
	`DES-7200(config-archive)# log config`
	`DES-7200(config-archive-log-config)# notify syslog`

Related commands

Command	Description
archive	Enter the archive configuration mode.
log config	Enter the archive log management configuration mode.
logging enable	Enable the function of logging the configuration change.

2.2 Showing and Monitoring Commands

2.2.1 show archive config differences

Use this command to compare the configurations in two specified configuration files line by line and output the configurations which are only existent in one of the configuration files.

show archive config differences [[*file1*] *file2*]

Parameter description

Parameter	Description
file1	The first configuration file name (including the path where the file is, it is optional)
file2	The second configuration file name (including the path where the file is, it is

	optional)

Default

If the *file1* and *file2* are both not specified, then assume the *file1* to the current configuration on the device and *file2* to the config.text file in the flash.

Command mode

Privileged mode.

Usage guidelines

By executing the **show archive config differences** command, users can see the configurations (the configurations here do not include the "!" in the configuration file) that only exist in one of the configuration files. The type of these configurations depends on the order of the specified configuration file. And in front of each configuration information, there is a identifier, which is used to identify the type of this configuraiton information. Compared with the *file1* , the identifiers and meanings are shown as below:

- With the "-" in front, the command does not exit in the *file2* but in the *file1*.
- With the "+" in front, the command exist in the *file2* but not in the *file1*.

Examples

The example following assumes that the content of the config_bak1.text and config_bak2.text are shown as below:

config_bak1.text	config_bak2.text
ip dhcp snooping verify mac-address ip dhcp snooping information option interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping suppression snmp-server host 1.1.1.1 traps public	ip dhcp snooping information option ip dhcp snooping bootp-bind interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping limit rate 1000 ip dhcp snooping

snmp-server enable traps	suppression snmp-server host 1.1.1.2 traps public snmp-server enable traps

The following example requires showing the configurations that exist in the config_bak2.text file but not in the config_bak1.text and the configurations that exist in the config_bak1.text file but not in the config_bak2.text.

```
DES-7200# show archive config differences flash:config_bak1.text flash:config_bak2.text
+ ip dhcp snooping bootp-bind
interface GigabitEthernet 0/3
 +ip dhcp snooping limit rate 1000
+snmp-server host 1.1.1.2 traps public
-ip dhcp snooping verify mac-address
-snmp-server host 1.1.1.1 traps public
```

Related commands

Command	Description
more *flash:config.text*	Show the content of the config.text file in the flash.
show archive config incremental-diffs	Show the entry list which is existent in the specified configuration file but not in the current configuration on the device.

2.2.2 show archive config incremental-diffs

Use this command to compare the configuration difference between the specified configuration file and the current device line by line, and output the configurations which is existent in the specified configuration file but not in the current device.

show archive config incremental-diffs [*file*]

Parameter description

Parameter	Description
file	Path and name of the specified configuration file.

Default

If the *file* is not specified, then assume it to the config.text file in the flash.

Command mode

Privileged mode.

Usage guidelines

By executing the **show archive config incremental-diffs** command, users can see the configurations (the configurations here do not include the "!" in the configuration file) that only exist in the specified configuration file but not in the current device.

Examples

The following example assumes that the configurations of the config_bak1.text file and current device are shown as below:

config_bak1.text	Configurations on current device
ip dhcp snooping information option ip dhcp snooping bootp-bind interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping limit rate 1000 ip dhcp snooping suppression snmp-server host 1.1.1.2 traps public snmp-server enable traps	ip dhcp snooping verify mac-address ip dhcp snooping information option interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping suppression snmp-server host 1.1.1.1 traps public snmp-server enable traps

The following example requires showing the configurations that exist in the config_bak1.text file but not in current device.

```
DES-7200# show archive config incremental-diffs config_bak1.text
ip dhcp snooping bootp-bind
interface GigabitEthernet 0/3
 ip dhcp snooping limit rate 1000
snmp-server host 1.1.1.2 traps public
```

	Command	Description
Related commands	**more** *flash:config.text*	Show the content of the config.text file in the flash.
	show archive config differences	Show the configuration differences between two specified configuration files.

2.2.3 show archive log config

Use this command to show the entry information of the configuraiton log.

show archive log config {{**all** | *start-num* [*end-num*]} [**provisioning** | **contenttype** [**plaintext**]] | **statistics**}

	Parameter	Description
Parameter description	**all**	Show all entry information of the configuration log.
	start-num [*end-num*]	Specifying the *start-num* means showing all configuration logs starting with this record. If the end-num is specified at the same time, it will show the configuration logs with the record number between the *start-num* and *end-num*. if the *start-num* is 0, it will show the configuration logs from the first entry. If the end-num is 0, it will show all configuration logs starting with the *start-num*. The *start-num* and *end-num* are both in the range of 0 to 2147483647.
	provisioning	Show the configuration logs in the format shown in the configuration file.
	contenttype	Specify the showing format of the configuration logs.
	plaintext	Specify the configuration logs to be shown in the ordinary text format.
	statistics	Show the memory usage of the configuration log.

Default	N/A.

Command mode

Privileged mode.

Usage guidelines

The *start-num* patameter must be specified when showing the configuration logs without the **all** specified. Use the *end-num* parameter to specify the range of the configuration logs to be viewed. When the configuration log entry that corresponding to the specified *end-num* is not existent, show all configuration logs from the *start-num* to the record number that is less than the *end-num*.(if the *end-num* is specified to 0, show all configuration logs starting with the *start-num*). On condition that the configuration log entry that corresponding to the specified *start-num* is not existent, show the configuration logs starting with the record number that is larger than the *start-num*. If the provisioning is specified, show the configuraitons in the format that is in the configuration files.

Examples

The following example shows the configuration logs numbered 1 to 2:

```
DES-7200# show archive log config 1 2
idx sess  user@line    datetime     logged command
1   1  unknown@console  Mar 21 09:57:22  | logging enable
2   1  unknown@console  Mar 21 09:57:46  | logging size 50
```

Field	Description
idx	The record number of the configuration log entry.
sess	Session number related to this configuration log entry.
user@line	Username and line name of generating this configuration log entry.
datetime	Time of generating this configuration log entry.
logged command	Executed configuration command.

The following example shows all configuration logs in the format of configurations shown in the configuration file.

```
DES-7200# show archive log config all provisioning
archive
 log config
  logging enable
  logging size 50
```

The following example shows the memory usage of the configuration log.

```
DES-7200# show archive log config statistics
Config Log Session Info:
  Number of sessions being tracked: 1
  Memory being held: 1270 bytes
  Total memory allocated for session tracking: 1270 bytes
  Total memory freed from session tracking: 0 bytes
Config Log log-queue Info:
 Number of entries in the log-queue: 3
  Memory being held in the log-queue: 671 bytes
  Total memory allocated for log entries: 671 bytes
  Total memory freed from log entries:: 0 bytes
```

Related commands

Command	Description
-	-

3 CPU-LOG Configuration Commands

3.1 Related System Management commands

3.1.1 show cpu

Use this command to show the CPU utilization information.

show cpu

Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to show the system CPU utilization information in 5sec, 1 min and 5 min, and the CPU utilization of every task in 5sec, 1 min and 5 min.

Examples

```
DES-7200# show cpu
=====================================
    CPU Using Rate Information
CPU utilization in five seconds: 25%
CPU utilization in one minute  : 20%
CPU utilization in five minutes: 10%
  NO   5Sec   1Min   5Min   Process
  0     0%     0%     0%    LISR INT
  1     7%     2%     1%    HISR INT
  2     0%     0%     0%    ktimer
  3     0%     0%     0%    atimer
  4     0%     0%     0%    printk_task
  5     0%     0%     0%    waitqueue_process
  6     0%     0%     0%    tasklet_task
  7     0%     0%     0%    kevents
  8     0%     0%     0%    snmpd
  9     0%     0%     0%    snmp_trapd
 10     0%     0%     0%    mtdblock
 11     0%     0%     0%    gc_task
 12     0%     0%     0%    Context
```

```
13    0%    0%    0%    kswapd
14    0%    0%    0%    bdflush
15    0%    0%    0%    kupdate
16    0%    3%    1%    ll_mt
17    0%    0%    0%    ll main process
18    0%    0%    0%    bridge_relay
19    0%    0%    0%    d1x_task
20    0%    0%    0%    secu_policy_task
21    0%    0%    0%    dhcpa_task
22    0%    0%    0%    dhcpsnp_task
23    0%    0%    0%    igmp_snp
24    0%    0%    0%    mstp_event
25    0%    0%    0%    GVRP_EVENT
26    0%    0%    0%    rldp_task
27    0%    2%    1%    rerp_task
28    0%    0%    0%    reup_event_handler
29    0%    0%    0%    tpp_task
30    0%    0%    0%    ip6timer
31    0%    0%    0%    rtadvd
32    0%    0%    0%    tnet6
33    2%    0%    0%    tnet
34    0%    0%    0%    Tarptime
35    0%    0%    0%    gra_arp
36    0%    0%    0%    Ttcptimer
37    8%    1%    0%    ef_res
38    0%    0%    0%    ef_rcv_msg
39    0%    0%    0%    ef_inconsistent_daemon
40    0%    0%    0%    ip6_tunnel_rcv_pkt
41    0%    0%    0%    res6t
42    0%    0%    0%    tunrt6
43    0%    0%    0%    ef6_rcv_msg
44    0%    0%    0%    ef6_inconsistent_daemon
45    0%    0%    0%    imid
46    0%    0%    0%    nsmd
47    0%    0%    0%    ripd
48    0%    0%    0%    ripngd
49    0%    0%    0%    ospfd
50    0%    0%    0%    ospf6d
51    0%    0%    0%    bgpd
52    0%    0%    0%    pimd
53    0%    0%    0%    pim6d
54    0%    0%    0%    pdmd
55    0%    0%    0%    dvmrpd
56    0%    0%    0%    vty_connect
```

```
  57    0%    0%    0%   aaa_task
  58    0%    0%    0%   Tlogtrap
  59    0%    0%    0%   dhcp6c
  60    0%    0%    0%   sntp_recv_task
  61    0%    0%    0%   ntp_task
  62    0%    0%    0%   sla_deamon
  63    0%    3%    1%   track_daemon
  64    0%    0%    0%   pbr_guard
  65    0%    0%    0%   vrrpd
  66    0%    0%    0%   psnpd
  67    0%    0%    0%   igsnpd
  68    0%    0%    0%   coa_recv
  69    0%    0%    0%   co_oper
  70    0%    0%    0%   co_mac
  71    0%    0%    0%   radius_task
  72    0%    0%    0%   tac+_acct_task
  73    0%    0%    0%   tac+_task
  74    0%    0%    0%   dhcpd_task
  75    0%    0%    0%   dhcps_task
  76    0%    0%    0%   dhcpping_task
  77    0%    0%    0%   dhcpc_task
  78    0%    0%    0%   uart_debug_file_task
  79    0%    0%    0%   ssp_init_task
  80    0%    0%    0%   rl_listen
  81    0%    0%    0%   ikl_msg_operate_thread
  82    0%    0%    0%   bcmDPC
  83    0%    0%    0%   bcmL2X.0
  84    3%    3%    3%   bcmL2X.0
  85    0%    0%    0%   bcmCNTR.0
  86    0%    0%    0%   bcmTX
  87    0%    0%    0%   bcmXGS3AsyncTX
  88    0%    2%    1%   bcmLINK.0
  89    0%    0%    0%   bcmRX
  90    0%    0%    0%   mngpkt_rcv_thread
  91    0%    0%    0%   mngpkt_recycle_thread
  92    0%    0%    0%   stack_task
  93    0%    0%    0%   stack_disc_task
  94    0%    0%    0%   redun_sync_task
  95    0%    0%    0%   conf_dispatch_task
  96    0%    0%    0%   devprob_task
  97    0%    0%    0%   rdp_snd_thread
  98    0%    0%    0%   rdp_rcv_thread
  99    0%    0%    0%   rdp_slot_change_thread
 100    4%    2%    1%   datapkt_rcv_thread
```

```
101     0%     0%     0%    keepalive_link_notify
102     0%     0%     0%    rerp_msg_recv_thread
103     0%     0%     0%    ip_scan_guard_task
104     0%     0%     0%    ssp_ipmc_hit_task
105     0%     0%     0%    ssp_ipmc_trap_task
106     0%     0%     0%    hw_err_snd_task
107     0%     0%     0%    rerp_packet_send_task
108     0%     0%     0%    idle_vlan_proc_thread
109     0%     0%     0%    cmic_pause_detect
110     1%     1%     1%    stat_get_and_send
111     0%     1%     0%    rl_con
112    75%    80%    90%    idle
```

In the list above, the first 3 lines indicates the system CPU utilization in 5sec, 1min and 5min, including LISR, HISR and task. Then, it describes the detailed CPU utilization distribution:

- No：Sequence number
- 5Sec：CPU utilization of the tasks in 5sec.
- 1Min：CPU utilization of the tasks in 1min.
- 5Min：CPU utilization of the tasks in 5min.

The first 2 lines in the list above indicate the CPU utilization of all LISRs and HISRs. From the 3rd line, it begins to refer to the CPU utilization of the tasks. The last line refers to the CPU utilization of the idle task, which is the same as the "System Idle Porcess" in the Windows. In the example above, CPU utilization of idle task within 5s is 75%, indicating that 75% CPU is idle.

3.1.2 cpu-log

Use this command to configure the low and high threshold of the cpu log utilization limit manually.

cpu-log *log-limit low_num high_num*

Parameter description

Parameter	Description
log-limit	The command descriptor prompting the log limit.
low_num	Set the low threshold of the cpu log utilization limit.
high_num	Set the high threshold of the cpu log utilization limit.

Default	By default, the high and low threshold of the cpu log utilization limit are 100% and 90%.
Command mode	Global configuration mode.
Usage guidelines	Use this command to configure the low and high threshold of the cpu log utilization limit manually. When the CPU using rate is more than the high threshold, it prompts the message; but if the CPU using rate exceeds the high threshold continuously, it only prompts the message for one time. When the CPU using rate is less than the low threshold, it prompts the message and advertises that the current CPU using rate has been down only when the CPU high and low threshold switches over.

Examples	This example shows how to set the low and high threshold of the cpu log utilization limit to 70% and 80% respectively.
	`DES-7200(config)# **cpu-log log-limit** *70 80*`
	The console prompts as follows when the CPU utilization rate is more than 80%:
	`Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute : 95% , Using most cpu's task is ktimer : 94%`
	The console prompts as follows when the CPU utilization rate is less than 70%:
	`Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute :68% , Using most cpu's task is ktimer : 60%`
	`Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: The CPU using rate has down!`

4 Memory Configuration Commands

4.1 Configuration Related Commands

4.1.1 memory-lack exit-policy

Use this command to set the exit-policy of the upper routing protocol when the memory reaches the lower threshold. The upper routing protocol includes BGP, OSPF, RIP and PIM-SM.

memory-lack exit-policy {**bgp** | **ospf** | **pim-sm** | **rip**}

no memory-lack exit-policy

Parameter description

Parameter	Description
bgp|ospf|pim-sm|rip	Specify the routing protocol: BGP, OSPF, PIM or RIP.
no	Restore to the default action.

Defaults

Exit from the routing protocol which occupies the largest memory.

Command mode

Global configuration mode.

Usage guidelines

When the memory size reaches the lower threshold (use the **show memory** command to show the lower threshold value), a routing protocol will be disabled to release the memory resources to ensure the operation of other protocols.

The user shall know that what routing protocols support the major services in the network. When the memory lacks, the user is able to disable the least important protocol to ensure the operation of major services.

For example, in a user network, BGP route is irrelevant to the network core services. The user can configure the BGP exit-policy when the memory lacks.

Specifying the disabled routing protocol to take precedence to exit the policy can not help the system obtain enough memory resources.

Note The exit-policy is used to protect the important network services to some degree when the system memory lacks. All routing protocols will exit and stop running if more memory resources are exhausted. 2 minutes later, the routing protocol will be attempting to restart.

Examples

This example shows how to enable the BGP to exit from the policy prior to other protocols:

```
DES-7200(config)# memory-lack exit-policy bgp
```

Related commands

Command	Description
show memory	Show the current memory usage information.

4.1.2 show memory

Use this command to show the current memory usage information.

show memory

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to view the current system memory state and usage information, including the system physical memory amount, the number of free pages in the current system, the free memory statistics.

Examples

This example shows the running result of the command **show memory**.

```
DES-7200#show memory
System Memory Statistic:
  Free pages: 1079
  watermarks : min 379, lower 758, low 1137, high 1516
  System Total Memory : 128MB, Current Free Memory : 5283KB
  Used Rate : 96%
```

The above information includes the following parts:

1. Free pages: the memory size of one free page is about 4k;
2. Watermarks(see the following table)

Parameter	Description
min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fails to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One routing protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the **memory-lack exit-policy** command.
low	The memory resources are insufficient. The routing protocol will be in OVERFLOW state if the low watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	The memory resources are sufficient. Each routing protocol attempts to restore the state from OVERFLOW to normal.

3. System total memory, current free memory and used rate.

4.1.3 show memory protocols

Use this command to display the usage of the memory for the routing protocols.

show memory protocols

Parameter description

Parameter	Description
None	-

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to display the usage of the memory for the routing protocols.

Note	Different switches and versions support different routing protocols. The main routing protocols are BGP, OSPF, RIP, LDP, PIM, ISIS, and ect.

Examples

This example shows the result of the command **show memory protocols**:

```
DES-7200(config)# show memory protocols
=================================================
protocol      |memory(byte)
BGP            102000000
OSPF            24000000
RIP             10000000
PIM             50000000
LDP             20000000
Total          206000000
```

Related commands

Command	Description
show memory	Show the current memory usage information.

5 POE Management Configuration Commands

5.1 Configurtion Related Command

POE configuration management includes the following related commands:

5.1.1 poe disconnect-mode mode

Use this command to set the disconnection detection mode. Use the **no** form of this command to restore to the default value.

poe disconnect-mode mode

no poe disconnect-mode

Parameter description	**Parameter**	**Description**
	mode	Disconnection detection mode, within the range of [ac/dc]
Command mode	Global configuration mode.	
Usage guidelines	This command is used to set the disconnection detection mode.	

Examples	Set the disconnect detection mode of the current POE system as **dc**:
	`DES-7200# configure`
	`DES-7200(config)# poe disconnect-mode dc`
	`DES-7200(config)# end`	

5.1.2 poe enable

Use this command to enable the POE(Power-over-Ethernet) function on the interface. Use the **no** form of this command to disable this function.

poe enable
no poe enable

Command mode	Global configuration mode.
Usage guidelines	Use this command to enable the POE function on the interface.
Examples	DES-7200(config-if)# DES-7200(config-if)# **poe enable** DES-7200(config-if)# **no poe enable** DES-7200(config-if)#

5.1.3 poe-power lower

Use this command to set the minimum allowed voltage. Use the **no** form of this command to restore to the default value.
poe-power lower *lower*
no poe-power lower

Parameter description	**Parameter**	**Description**
	lower	Minimum allowed voltage, within the range [45000 to 47000] mv.

Command mode	Global configuration mode.
Usage guidelines	This command is used to set the minimum allowed voltage.
Examples	The following example sets the minimum allowed voltage of the current POE system as 46000 mv. DES-7200# **configure** DES-7200(config)# **poe-power lower** *46000* DES-7200(config)# **end**

5.1.4 poe-power upper *upper*

Use this command to set the maximum allowed voltage. Use the **no** form of this command to restore to the default value.
poe-power upper *upper*
no poe-power upper

Parameter description

Parameter	Description
upper	Maximum allowed voltage, within the range [55000 to 57000] mv.

Command mode Global configuration mode。

Usage guidelines This command is used to set the maximum allowed voltage.

Examples The following example sets the maximum allowed voltage of the current POE system as 56000 mv.

```
DES-7200# configure
DES-7200(config)# poe-power upeer 56000
DES-7200(config)# end
```

5.2 Show Related Command

5.2.1 show poe interface(s)

Use this command to view the POE status of the interface.

show poe interface(s) [*interface-id*]

Command mode Privileged EXEC mode.

Usage guidelines This command is used to view the POE status of the specified interface or all interfaces.

Examples

```
DES-7200# show poe interface gigabitethernet 0/2
Interface : Gi0/2
Port power enabled : ENABLE
Port connect status : OFF
Port PD Class : no PD devices
Port max power : 15400 mW
Port current power : 0 mW
Port peak power : 0 mW
Port current : 0 mA
```

```
Port voltage : 48082 mV
Port trouble cause : normal


DES-7200# show poe interfaces
Interface  Power   Link    Max   Curr   Peak   Curr   Trouble
Pd    Port
      Control  Status  Power  Power  Power  Icut   Cause
Class  Voltage
-------------------------------------------------------------
------------
Gi0/1     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/2     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/3     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/4     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/5     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/6     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/7     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/8     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/9     Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/10    Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/11    Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
Gi0/12    Disable  OFF    0.0W   0.0W   0.0W   0mA   normal
0     0.0V
```

5.2.2 show poe powersupply

Use this command to view the POE power supply status.

show poe powersupply

Command mode	Privileged EXEC mode.

Usage guidelines	This command is used to view the POE power supply status.
Examples	DES-7200# **show poe powersupply** PSE Total Power : 379971 mW PSE Total Power Consumption : 0 mW PSE Available Power : 379971 mW PSE Peak Value : 0 mW PSE Min Allow Voltage : 45000 mV PSE Max Allow Voltage : 57000 mV PSE Disconnect Sense Mode : ac

6 Syslog Configuration Commands

6.1 Related Configuration Commands

6.1.1 clear logging

Use this command to clear the logs from the buffer.

clear logging

Command mode	Privileged EXEC mode.
Usage guidelines	This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.
Examples	The following example clears the log packets from the memory buffer. `DES-7200# clear logging`

Related commands

Command	Function
logging on	Record logs on different devices.
show logging	Show the logs in the buffer.
logging buffered	Record the logs to the memory buffer.

6.1.2 logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs. The **no** form of the command disables recording logs in memory buffer. The **default** form of this command restores the memory buffer size to the default value.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

Parameter description

Parameter	Description
buffer-size	Size of the buffer is related to the specific device: For the kernel / aggregation switches, 4K to 10M bytes. For the access switches, 4K to 1M. For other devices, 4K to 128K Bytes.
level	Severity of logs, 0 to 7. The name of the severity or the numeral can be used.

Default configuration

The buffer size is related to the specific device type.

1. kernel switches: 1M Bytes;
2. aggregation switches: 256K Bytes;
3. access switches: 128K Bytes;
4. other devices: 4K Bytes

The log severity is 7.

Command mode

Global configuration mode.

Usage guidelines

The memory buffer for log is used in recycled manner. That is, when it is full, the oldest information will be overwritten. To show the log information in the memory buffer, run **show logging** at the privileged user level.

The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of command **clear logging** by privileged user. To trace a problem, it is required to record logs in flash or send them to Syslog Server.

The log information of the DES-7200 is classified into the following 8 levels:

Table-1

Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy

Critical	2	Critical conditions
Errors	3	Error message
warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
informational	6	Descriptive information
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level.

When the level of log information to be displayed on specified device, the log information is at or below the set level will not be displayed.

Caution

After running the system for a long time, modifying the log buffer size especially in condition of large buffer may fails due to the insufficent availble continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.

Examples

The configuration example below allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes.

```
DES-7200(config)# logging buffered 10000 6
```

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs in the buffer.
clear logging	Clear the logs in the log buffer.

6.1.3 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console. The **no** format of the command disables displaying the logs on the console.

logging console *level*

no logging console

Parameter description

Parameter	Description
level	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 60-1.

Default configuration Debugging (7).

Command mode Global configuration mode.

Usage guidelines

When a log severity is set here, the log messages at or below that severity will be displayed on the console.

The **show logging** command displays the related setting parameters and statistics of the log.

Examples

The example below sets the severity of log that is allowed to be displayed on the console as 6:

```
DES-7200(config)# logging console informational
```

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.

6.1.4 logging count

Use this command to enable the log statistics function. The **no** format of the command deletes the log statistics and disables the statistics function.

logging count

no logging count

Parameter description N/A.

Default configuration Disabled.

Command mode Global configuration mode.

Usage guidelines	This command enables the log statistics function. The statistics begins when the function is enabled. If you run **no logging count**, the statistics function is disabled and the statistics data is deleted.
Examples	Enable the log statistics function: `DES-7200(config)# logging count`

Related commands

Command	Description
show logging count	Show the log statistics.
show logging	Show the logs and related log configuration parameters in the buffer.

6.1.5 logging facility

Use this command to configure the log device. The **no** format of the command restores it to the default device value (23).

logging facility *facility-type*

no logging facility

Parameter description

Parameter	Description
facility-type	Syslog device value. For detailed configuration value, refer to the usage guidelines.

Default configuration	Local7(23).
Command mode	Global configuration mode.

Usage guidelines

The following table (Table-2) is the possible device value of Syslog:

Table-2

Numerical Code	Facility
0 (kern)	Kernel messages

1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization message
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer system
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization message
11 (ftp)	FTP daemon
12 (ntp)	NTP daemon
13 (logaudit)	Log audit
14 (logalert)	Log alert
15 (clock2)	Clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

The default device value of DES-7200 is 23 (local 7).

Examples

Following is to set the device value of **Syslog** as **kernel**:

```
DES-7200(config)# logging facility kern
```

Related commands

Command	Description
logging console	Set the severity of logs that are allowed to be displayed on the console.

6.1.6 logging file flash

Use this command to record logs in the flash. The **no** format of the command disables the function.

logging file flash:*filename* [*max-file-size*] [*level*]

no logging file

Parameter description

Parameter	Description
filename	Name of the log file of txt type
max-file-size	Maximal size of the log file in the range 128K to 6M bytes, 128K bytes by default
level	The severity of logs recorded in the log files. The name of the severity or the numeral can be used. By default, the severity of logs recorded in the FLASH is 6. For the details of log severity, please see Table-1.

Default configuration

Logs are not recorded in the FLASH.

Command mode

Global configuration mode.

Usage guidelines

If no **Syslog Server** is specified or it is not desired to transfer logs in the network due to the consideration of security purpose, it is possible to save the logs directly in flash.

The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.

To record the logs into the expansion FLASH, The expansion FLASH is required. If there is no expansion FLASH, the logging file flash will be hidden automatically and the related configuration will be denied.

Caution

Each syslog file has the limitation of the maximum length. Before writing a new syslog to a file, the followings help determine whether the maximum length of the file has been exceeded:

A new syslog file will be created if the

	maximum length has been exceeded; Add a number to the name of the new file based on the original filename, in the format of filename_number with the suffix txt. The maximum number is 15. The first file will be overwritten if the number reaches 15. Therefore, up to 16 files will be generated in the FLASH when configuring the command to write one syslog to the FLASH.

Examples	The example below records the logs into the expansion FLASH, with the name trace.txt, file size 128K and log severity 6. `DES-7200(config)# logging file flash:trace`

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.
more flash	View the logs in the flash.

6.1.7 logging monitor

Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.). The **no** format of the command disables displaying the logs on the VTY window.

logging monitor *level*

no logging monitor

Parameter description

Parameter	Description
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1.

Default configuration	Debugging (7).

Command mode	Global configuration mode.
Usage guidelines	To print log messages on the VTY window, execute first the privileged user command **terminal monitor**. The level of logs to be displayed is defined with **logging monitor**. The log level defined with "Logging monitor" is for all VTY windows.
Examples	The example below sets the severity of log that is allowed to be printed on the VTY window as 6: `DES-7200(config)# logging monitor informational`

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.

6.1.8 logging on

Use this command to record logs on different devices. The **no** form of this command disables the fucntion.

logging on
no logging on

Parameter description	N/A
Default configuration	Logs are allowed to be displayed on different devices.
Command mode	Global configuration mode.
Usage guidelines	DES-7200 can not only show the log information in the Console window and VTY window, but also record it in different equipments such as the memory buffer, the FLASH and Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is greater than 1.

Examples	The following example disables the log switch in the equipment. `DES-7200(config)# no logging on`

Related commands	**Command**	**Description**
	logging buffered	Record the logs to an internal buffer.
	logging	Record logs to the Syslog server.
	logging file flash:	Record logs on the FLASH.
	logging console	Set the log level to be displayed on the console.
	logging monitor	Set the log level to be displayed on the VTY window (such as telnet window) .
	logging trap	Set the log level to be sent to the Syslog server.

6.1.9 logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. The **no** form of this command disables log rate limit function.

logging rate-limit {*number* | **all** *number* | **console** {*number* | **all** *number*}} [**except** *severity*]

no logging rate-limit

Parameter description	**Parameter**	**Description**
	number	The number of logs processed in a second with the range from 1 to 10000.
	all	Set rate limit to all the logs with severity level 0-7.
	console	Set the amount of logs shown in the console in a second.
	except	By default, the severity level is error(3). The rate of the log whose severity level is less than or equal to this severity level is not controlled.
	severity	Log severity level with the range from 0 to 7. The lower the level is, the higher the severity is.

Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Use this command to control the syslog outpt to prevent the massive log output.
Examples	The example below sets the number of the logs (including debug) processed in a second as 10. However, the logs with warning or higher severity level are not controlled: `DES-7200(config)#logging rate-limit all 10 except warnings`

Related commands

Command	Description
show logging count	Show the log statistics.
show logging	Show the logs and related log configuration parameters in the buffer.

6.1.10 logging server

Use this command to record the logs in the specified Syslog sever. The **no** form of the command deletes the Syslog server with specified address from the Syslog server list.

logging server {*ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address*}

no logging server {*ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address*}

Parameter description

Parameter	Description
ip-address	Receive IP address of the log server.
vrf-name	Specify VRF (VPN device forwarding list) connecting to the log server.
ipv6-address	Specify IPV6 address of the log server.

Default configuration	By default, it does not send the logs to any syslog server.

Command mode	Global configuration mode.
Usage guidelines	This command specifies a Syslog server to receive the logs of the device. The DES-7200 allows the configuration of up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

Examples	The example below specifies a syslog server at address 202.101.11.1:
	`DES-7200(config)# logging server 202.101.11.1`
	The example below specifies an ipv6 address as AAAA:BBBB:FFFF:
	`DES-7200(config)# logging server ipv6 AAAA:BBBB:FFFF`

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.
logging trap	Set the level of logs to be sent to Syslog server.

6.1.11 logging source interface

Use this command to configure the source interface of logs. The **no** format of the command cancels the source interface setting for the specified log.

logging source interface *interface-type interface-number*

no logging source interface

Parameter description

Parameter	Description
interface-type	The type of interface
interface-number	The number of interface

Default configuration	N/A.
Command mode	Global configuration mode.

Usage guidelines	By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique address. If no source interface of the device or no IP address of the source interface is configured, the source IP address of the log message is still that of the interface from which the message is sent.
Examples	The example below specifies loopback 0 as the source address of the syslog messages: `DES-7200(config)# logging source interface loopback 0`

Related commands

Command	Description
logging	Record logs to the Syslog server.

6.1.12 logging source ip| ipv6

Use this command to configure the source IP address of logs. The **no** format of the command cancels the source IP address setting for the specified log.

logging source {**ip** *ip-address* **| ipv6** *ipv6-address*}

no logging source {**ip | ipv6**}

Parameter description

Parameter	Description
ip-address	Specify the source IPV4 address sending the logs to IPV4 log server.
ipv6-address	Specify the source IPV6 address sending the logs to IPV6 log server.

Default configuration	N/A.
Command mode	Global configuration mode.

Usage guidelines	By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique address. If no IP address is configured for the device, the source IP address of the log message is still that of the interface from which the message is sent.
Examples	The example below specifies the 192.168.1.1 as the source address of the syslog messages: `DES-7200(config)# logging source ip 192.168.1.1`

Related commands

Command	Description
logging	Record logs to the Syslog server.

6.1.13 logging synchronous

Use this command to enable synchronization function of user input and log output in the line configuration mode to prevent the user from interrupting when keying in the characters. The **no** form of this command disables this function.

logging synchronous

no logging synchronous

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Line configuration mode.
Usage guidelines	This command enables synchronization function of user input and log output, preventing the user from interrupting when keying in the characters.
Examples	`DES-7200(config)#line console 0` `DES-7200(config-line)#logging synchronous`

Print UP-DOWN logs on the port when keying in the command, the input command will be output again:

```
DES-7200#configure terminal
Oct 9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down
Oct 9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to DOWN
DES-7200#configure terminal ----the input command by the user is output again rather than being intererupted.
```

Related commands

Command	Description
show running-config	View the configuration.

6.1.14 logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server. The **no** format of the command disables sending the logs to the syslog server.

logging trap *level*

no logging trap

Parameter description

Parameter	Description
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 60-1.

Default configuration

Informational(6).

Command mode

Global configuration mode.

Usage guidelines

To send logs to the Syslog Server, execute first the global configuration command **logging** to configure the **Syslog Server**. Then, execute **logging trap** to specify the severity of logs to be sent.

The **show logging** command displays the related setting parameters and statistics of the log.

Examples

The example below enables logs at severity 6 to be sent to the Syslog Server at address 202.101.11.22:

```
DES-7200(config)# logging 202.101.11.22
DES-7200(config)# logging trap informational
```

Related commands

Command	Description
logging on	Reocrd logs on different devicds.
logging	Record logs to the Syslog server.
show logging	Show the logs and related log configuration parameters in the buffer.

6.1.15 more flash

Use this command to show the contents of the logs stored in the FLASH.

more flash:*filename*

Parameter description

Parameter	Description
filename	Log file name

Command mode

Privileged EXEC mode.

Usage guidelines

In the FLASH, the log file means the files with the prefix "//f2/", "//f3/'. This command only allows you to view the log files. You cannot use this command to view other non-log files.

Examples

The following example shows the results of the log files in the FLASH as you can see:

```
DES-7200# more flash://f2/log.txt
look up file in the extended flash://f2/log.txt
00004 2004-11-17 4:1:32 DES-7200: %5:Reload requested by Administrator. Reload Reason :Reload command
```

Related commands

Command	Function
logging file flash	Record the logs to the FLASH.

6.1.16 service sequence-numbers

Use this command to attach sequential numbers into the logs. The **no** format of the command removes the sequential numbers in the logs.

service sequence-numbers
no service sequence-numbers

Parameter description	N/A.
Default configuration	No sequential numbers are attached.
Command mode	Global configuration mode.
Usage guidelines	In addition to the timestamp, it is possible to add sequential numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.
Examples	The example below adds sequential numbers to the logs. `DES-7200(config)# service sequence-numbers`

Related commands

Command	Description
logging on	Record logs on different devices.
service timestamps	Attach the timestamp to the logs

6.1.17 service sysname

Use this command to attach system name to logs. The **no** format of the command removes the system name from the logs.

service sysname
no service sysname

Parameter description	N/A.
Default configuration	No system name is attached.
Command mode	Global configuration mode.

Usage guidelines	This command allows you to decide whether to add system name in the log information.

Examples

Add system name in the log information:

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by
console
DES-7200 #config terminal
Enter configuration commands, one per line. End with
CNTL/Z.
DES-7200 (config)#service sysname
DES-7200 (config)#end
DES-7200 #
```

Mar 22 15:35:57 DES-7200 %SYS-5-CONFIG: Configured from console by console

Related commands

Command	Function
show logging	Show the logs and related log configuration parameters in the buffer.

6.1.18 service timestamps

Use this command to attach timestamp into logs. The **no** format of the command removes the timestamp from the logs. The **default** format of this command restores the timestamp configuration to the defalt.

service timestamps [*message-type* [**uptime** | **datetime** [**msec** | **year**]]]

no service timestamps [*message-type*]

default service timestamps [*message-type*]

Parameter description

Parameter	Description
message-type	The type of log, including **Log** and **Debug**. The **log** type means the log information with severity levels of 0 to 6. The **debug** type means that with severity level 7.
uptime	Device start time in the format of *Day*Hour*Minute*Second, for example, 07:00:10:41
datetime	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07

msec	Current time of the device in the format of Month*Date*Hour*Minute*Second*millisecond, for example, Jul 27 16:53:07.299
year	Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07

Default configuration

The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.

Command mode

Global configuration mode.

Usage guidelines

When the uptime option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the datetime option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.

Examples

The example below enables the timestamp for **log** and **debug** information, in format of Datetime, supporting millisecond display.

```
DES-7200(config)# service timestamps debug datetime msec
DES-7200(config)# service timestamps log datetime msec
DES-7200(config)# end
DES-7200(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I:
configured from console by console
```

Related commands

Command	Description
logging on	Record logs on different devices.
service sequence-numbers	Attach sequential number to logs.

6.1.19 terminal monitor

Use this command to show logs on the current VTY. The **no** form of this command is used to disable the function.

terminal monitor

terminal no monitor

Default

By default, no logs are displayed on the VTY window.

configuration	
Command mode	Privileged EXEC mode.
Usage guidelines	This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is lost. This command can also be run on the console, but it does not take effect.
 **Note**	For easy management, the DES-7200 allows the use the command on the console. The **no** form of the command executed on the console allows only the emergent log messages with severities 0 and 1.

Examples	The example below allows log information to be printed on the current VTY window.
	`DES-7200# terminal monitor`
	`DES-7200#`

6.2 Showing Related Commands

6.2.1 show logging

Use this command to show parameters and statistics information about logs and the logs in the buffer.

show logging

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A
Examples	The following command shows the result of the show logging command:

```
DES-7200# show logging
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487:  *Sep  19  02:46:13:  DES-7200  %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015488: *Sep 19 02:46:13: DES-7200 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up.
015489:  *Sep  19  02:46:26:  DES-7200  %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.
015490: *Sep 19 02:46:26: DES-7200 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to down.
015491:  *Sep  19  02:46:28:  DES-7200  %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015492: *Sep 19 02:46:28: DES-7200 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up.
```

The log messages are described as below:

Field	Description
Syslog logging	Logging switch: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics

Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics
Standard format	Standard log format
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence log messages	Sequence switch
Sysname log messages	System name added to the log messages
Count log messages	Log statistical function.
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

Related commands

Command	Function
logging on	Record logs on different devices.
clear logging	Clear the logs in the buffer.

6.2.2 show logging count

Use this command to show the log statistics.

show logging count

Parameter description

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

To use the log packet statistics function, run **logging count** in the global configuration mode. The **show logging count** can show the information of a log, occurrence times, and the last occurrence time.

You can use **show logging** to check whether the log statistics function is enable.

Examples

The following is the execution result of **show logging count**:

```
DES-7200# show logging count
Module Name   Message Name Sev Occur     Last Time
SYS          CONFIG_I        5   1        Jul 6 10:29:57
SYS TOTAL                        1
```

Related commands

Command	Function
logging count	Enable the log statistics function.
show logging	Show the logs and related log configuration parameters in the buffer.
clear logging	Clear the logs in the buffer.

7 Module Hot-plugging/ unplugging Configuration Commands

7.1 Related Configuration Commands

7.1.1 install slot-num moduletype

Use this command to install the module driver manually.

install *slot-num moduletype*

Parameter description

Parameter	Description
slot-num	Slot number.
moduletype	Module type

Command mode

Global configuration mode.

Usage guidelines

This command is used to install the module driver manually. After the installation, all configurations for the slot will be done for the type of the installed module. Even if the module is unplugged, you can still configure it without loss of the configuration.

Examples

Install module 24SFP/12GT in slot 2

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
DES-7200(config)# install 2 24SFP/12GT
2006-04-22 09:26:00  @5-CONFIG:Configured from outband
DES-7200(config)# end
DES-7200# show version module detail 2
Device  : 1
Slot    : 2
User Status  : installed
```

```
Software Status: none
Online Module :
Type  :
Ports   : 0
Version :
Configured Module :
Type  : M8606-24SFP/12GT
Ports   : 24
Version :
```

Related commands

Command	Description
no install slot-num	Uninstall the module in the slot.
show version module detail	Show the detailed information of a module.
show version slots	Show slot details

7.1.2 no install slot-num

Use this command to unistall the module manually.

no install *slot-num*

Parameter description

Parameter	Description
slot-num	Slot number.

Command mode

Global configuration mode.

Usage guidelines

Use this command to uninstall a module. Once uninstalled, all configurations for that module will be lost and the module will be deactivated, unless you manually install the driver for the module.

Examples

Uninstall module 24SFP/12GT in slot 2

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
DES-7200(config)# no install 2
2006-04-22 09:26:00  @5-CONFIG:Configured from outband
DES-7200(config)#end
DES-7200# show version module detail 2
Device  : 1
Slot    : 2
```

```
User Status  : none
Software Status: none
Online Module :
Type  :
Ports   : 0
Version :
Configured Module :
Type  :
Ports   :
Version :
DES-7200#
```

Related commands

Command	Description
install slot-num *moduletype*	Install a module in the slot.
show version slots	Show slot details.

7.1.3 remove configuration module slot-num

Use this command to remove the module configurations.

remove configuration module *slot-num*

Parameter description

Parameter	Description
slot-num	Slot number.

Command mode

Global configuration mode.

Usage guidelines

Use this command to remove the module configurations. If there is a module inserted in the slot, this module will be reset.

Examples

```
DES-7200(config)# remove configure module 4
```

7.1.4 reset module slot-num

Use this command to reset a module.

reset module *slot-num*

Parameter description

Parameter	Description
slot-num	Slot number.

Command mode

Privileged EXEC mode

Usage guidelines

Use this command to reset a module.

Examples

```
DES-7200# reset module 4
```

7.2 Showing Related Command

7.2.1 show version module detail [*module-num*]

Use this command to show the details of the module.

show version module detail [*module-num*]

Parameter description

Parameter	Description
module-num	(Optional) Module number.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to show details of the module

Examples

```
DES-7200# show version module detail 2
Device  : 1
Slot    : 2
User Status :    none
Software Status: none
Online Module :
Type  :
Ports   : 0
Version :
Configured Module :
Type  :
Ports   :
Version :
DES-7200#
```

Related commands	**Command**	**Description**
	show version slots	Show slot details.

7.2.2 show version slots [slot-num]

Use this command to view the details of the slot.

show version slots [*slot-num*]

Parameter description	**Parameter**	**Description**
	num	(Optional) Slot number.

Command mode	Privileged EXEC mode.

Examples

```
DES-7200# show version slots
Dev Slot  Configured Module Online Module  User Status
Software Status
--- ----  -----------------   -----  --------------
1 1    none         none
1 2 M8606-24SFP/12GT M8606-24SFP/12GT installed none
1 3 M8606-2XFP M8606-2XFP uninstalled  cannot startup
1 4 M8606-24GT/12SFP M8606-24GT/12SFP installed ok
1 M1 M8606-CM   M8606-CM              master
1   M2                                 none
```

Related commands	**Command**	**Description**
	show version moduel detail	Show the details of the module.

8 LCD Configuration Commands

8.1 Related Configuration Commands

8.1.1 lcd language

Use this command to configure the language displayed on the LCD . Use the **no** form of this command to restore the default value.

lcd language { **chinese** | **english** }

no lcd language

Parameter description

Parameter	Description
chinese	Set the language displayed on the LCD to Chinese.
english	Set the language displayed on the LCD to English.

Default configuration

The default displaying language is Chinese except for some customized products.

Command mode

Global configuration mode

Usage guidelines

Use this command to change the language displayed on the LCD.

Examples

The following example configures the language displayed on the LCD to English.

```
DES-7200(config)# lcd language english
```

Platform description

This command is supported on the DES-7200 series only.

8.1.2 lcd trap-number num

Use this command to configure the length of alarm messages. Use the **no** form of this command to restore the default value.

lcd trap-number *num*

no lcd rap-number

Parameter description

Parameter	Description
num	An integer in the range of 1 to1000.

Default configuration The default value is 100.

Command mode Global configuration mode

Usage guidelines Use this command to view the recently generated alarms. By default, 100 latest alarms are displayed. You can use this command to change the number of the latest alarms displayed.

Examples The following example shows 200 latest alarms.

```
lcd trap-num 200
```

8.1.3 memory-rate rising-threshold num

Use this command to set the value of memory-rate rising-threshold.

memory-rate rising-threshold *num*

Parameter description

Parameter	Description
num	An integer in the range of 1 to 100.

Default configuration The default value is 80.

Command mode Global configuration mode.

Usage guidelines If the num is 80, the result of show running-config does not show the memory-rate rising-threshold *80.*

Examples

```
DES-7200(config)# memory-rate rising-threshold 60
```

Platform description

This command is supported on the DES-7200 series only.

9 USB/SD configuration Commands

9.1 Related Configuration Commands

The commands described here are used to query and remove USB/SD devices in the CLI environment in the main program.

9.1.1 show usb

Use this command to show the information about the inserted USB device in the system.

show usb

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Device information is displayed if there is a USB device. Otherwise, there is no output.

Examples	The following example shows the information about the USB device:
	`DES-7200# show usb`
	`Device: Mass Storage:`
	`ID: 0`
	`URL prefix: usb0`
	`Disk Partitions:`
	`usb0(type:FAT32)`
	
	`Size : 131,072,000B(125MB)`
	`Available size: 1,260,020B (1.2MB)`
	In above information, the Mass Storage Device is the name of the device.
	The meaning of the information is as below:

Table 1: the description of the field .

Field	Description
URL	Prefix used to access the USB device.
Size	Accessible size of the USB device.
Available size	Available size of the USB device.

9.1.2 show sd

Use this command to show the information about the inserted SD device in the system.

show sd

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines Device information is displayed if there is a SD device. Otherwise, there is no output.

Examples

The following example shows the information about the SD device:

```
DES-7200# show sd
          Device: Mass Storage:
          ID: 1
          URL prefix: sd0
          Disk Partitions:
          SD(type:FAT32)
          Size : 131,072,000B(125MB)
        Available size：  1,260,020B（1.2MB）
```

In above information, the Mass Storage Device is the name of the device.

The meaning of the information is as below:

Table 1: the description of the field .

URL	Prefix used to access the SD device.
Size	Accessible size of the SD device.

9.1.3 sd remove

sd remove *device_id*

Parameter description

Parameter	Description
device_id	Device ID of SD to be removed.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines Before pulling out the SD device, you need to remove the device using a command, so as to prevent errors that may occur because the system is using the device. If the device is removed successfully, the system will show a prompt, when you can pull out the device. If the device cannot be pulled out, it indicates that the system is using this SD device, so you have to wait a moment before removing it again.

Examples The following example demonstrates how to remove the SD device mentioned in the example in the previous section.

```
DES-7200# sd remove 1

OK, now you can pull out the device 1.
```

At this moment, the SD card can be plugged out.

9.1.4 usb remove

usb remove *device_id*

Parameter description

Parameter	Description
device_id	Device ID of USB to be removed.

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Before pulling out the USB device, you need to remove the device using a command, so as to prevent errors that may occur because the system is using the device. If the device is removed successfully, the system will show a prompt, when you can pull out the device. If the device cannot be pulled out, it indicates that the system is using this USB device, so you have to wait a moment before removing it again.

Examples	The following example demonstrates how to remove the USB device mentioned in the example in the previous section.
	`DES-7200# usb remove 0`
	`OK, now you can pull out the device 0.`
	`*Jan 1 00:18:16: %USB-5-USB_DISK_REMOVED: USB Disk <Mass Storage> has been removed from USB port 0!`
	At this moment, the USB device can be plugged out.