xStack DGS-3610 Series

CLI Reference Guide

Version 10.2

D-Link®

DGS-3610 Series CLI Reference Guide

Revision No.: Version 10.2

Date:

Preface

Version Description

This manual matches the Firmware version v10.2.

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.

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 characters in bold.

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

[ ]: The part enclosed with [ ] is 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.

//: A line starting with a double slash "//" is a comment line.

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

 **Note**	The port types described in the examples in this manual may not be consistent with the actual types. During actual operations, configuration should be made according to the type of ports supported by various products. The display information in some examples in this manual may include the content of other product series (such as the product model and description). For the concrete display information, refer to actual equipment information used.

Contents

1 Configuring CLI Authorization Command

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 specified alias of a command or all the aliases within one mode.

alias *mode command-alias original-command*
no alias *mode [original-command]*

Parameter description

Parameter	Description
mode	Mode of the command represented by the alias.
command-alias	Alias of the command.
original-command	Actual syntax of the command represented by the alias

Default configuration

Some commands in the 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 EXEC mode.

Alias	Actual Command
h	**help**
p	**ping**
s	**show**
u	**undebug**
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 command modes that allow for setting of alias.

```
DGS-3610(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, which is displayed after * in the following format:

**command-alias=original-command*

For example, in the 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.

```
DGS-3610# 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” for “**show version**” in the EXEC mode, then:

```
DGS-3610# 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.

```
DGS-3610# 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:

```
DGS-3610(config-if)# ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
DGS-3610(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 command of “ip router 0.0.0.0 0.0.0.0 192.168.1.1“**:**

```
DGS-3610# configure terminal
DGS-3610(config)# alias config def-route ip route 0.0.0.0 0.0.0.0
192.168.1.1
DGS-3610(config)# def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
DGS-3610(config)# def-route?
% Unrecognized command.
DGS-3610(config)# end
DGS-3610# 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 grant the execution rights of a command to a command level, use **privilege** in the global configuration mode. The **no** form of this command resets the execution rights of a command to the default setting.

privilege *mode* [**all] {leve**l *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 authorized
[all]	All the right of the sub-commands will be specified as the same right level.
level level	Specify the execution right levels (0–15) of a command or sub-commands.
reset	Reset the command execution rights to its default level.
command-string	Command string to be authorized.

Default configuration

None.

Command mode

Global configuration mode.

Usage guidelines

The following table lists some key words that can be authorized in the **privilege** command 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 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 to "**test**" and set the right to perform the **reload** command to reset the device:

```
DGS-3610(config)# enable secret level 1 0 test
DGS-3610(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：

```
DGS-3610> reload ?
  <cr>
```

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

```
DGS-3610(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:

```
DGS-3610> 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 **show aliases** in the EXEC mode.

show aliases [*mode*]

Parameter description

Parameter	Description
mode	Mode of the command represented by the alias

Default configuration

None.

Command mode

EXEC mode.

Usage guidelines

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

Examples

The following example shows the command alias in the EXEC mode:

```
DGS-3610# 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 Configuring Switch Management Command

2.1 User Management Related Commands

The user interface is the user command line interface (CLI), including the following related commands:

- **disable**
- **enable**
- **enable password**
- **enable secret**
- **password**
- **login**
- **login local**
- **login authentication**
- **username**
- **lock**
- **lockable**
- **telnet**
- **enable service**

2.1.1 disable

To exit from privileged user mode to normal user mode or lower to 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 router down to level 10:

```
DGS-3610# disable 10
```

Related commands

Command	Description
enable	From general 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 general user configuration command **enable**.

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

2.1.3 enable password

To configure the passwords for different privilege levels, 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

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 only when the password of the command that has been encrypted by the router is copied and pasted. A valid password is defined as follows: ■ Consists of 1 ~ 26 letter in upper/lower case and numerals ■ Leading spaces are allowed but ignored. Spaces in between or at the end are regarded a part of the password.  **Caution** If an encryption type is specified and then a plaintext password is entered, it is impossible to enter the privileged mode. A lost password that has been encrypted with any method cannot be restored. The only way is to reconfigure the router password.
Examples	The example below configures the password as **pw10**: `DGS-3610(config)# enable password pw10`

Related commands

Command	Description
enable secret	Set the security password

2.1.4 enable secret

To configure security passwords for different privilege levels, 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 levels 0 ~ 15. If both types of passwords exist in the system, the password of **password** type will not take effect. If a password of the **password** type is set for a level other than 15, an alert is provided and the password is automatically converted into the **security** password. If a password of the **password** type is set for level 15 and is 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: `DGS-3610(config)# enable secret 0 pw10`

Related commands

Command	Description
enable password	Set passwords for different privilege levels.

2.1.5 password

To configure the password for line logon, execute 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:**:
	`DGS-3610(config)# line vty 0`
	`DGS-3610(config-line)# password red`

Related commands

Command	Description
login	Exit from the user mode and enter the privileged mode, or log on to the higher level of authority.

2.1.6 login

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

login

no login

Parameter description	No parameters
Command mode	line configuration mode.
Usage guidelines	If the AAA security server is not enabled, this command is used for the simple password verification 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 verification on VTY.
	`DGS-3610(config)# no aaa new-model`
	`DGS-3610(config)# line vty 0`
	`DGS-3610(config-line)# password 0 normatest`
	`DGS-3610(config-line)# login`

Related commands

Command	Description
password	Configure the line logon password

2.1.7 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	No parameters
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.
	`DGS-3610(config)# no aaa new-model`
	`DGS-3610(config)# username test password 0 test`
	`DGS-3610(config)# line vty 0`
	`DGS-3610(config-line)# login local`

Related commands

Command	Description
username	Configure the local user information.

2.1.8 login authentication

In case the AAA is enabled, the authentication with the AAA server must be performed for logon. This command is used 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	The default authentication method list.
list-name	The optional 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.
	`DGS-3610(config)# aaa new-model`
	`DGS-3610(config)# aaa authentication login default radius`
	`DGS-3610(config)# line vty 0`
	`DGS-3610(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

2.1.9 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 a 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 binds the user to level 15.

```
DGS-3610(config)# username test privilege 15 password 0 pw15
```

Related commands

Command	Description
login local	Enable local authentication

2.1.10 lock

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

lock

Parameter description

None

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 performing 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 re-enter the terminal again, input the set temporary password.

To use the terminal locking function on the terminal, execute the **lockable** command in the line configuration mode, and enable the feature to support the terminal lock in corresponding line.

Examples

The example below locks a terminal interface:

```
DGS-3610(config-line)# lockable
DGS-3610(config-line)# end
DGS-3610# lock
Password: <password>
Again: <password>
Locked
Password: <password>
DGS-3610#
```

Related commands

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

2.1.11 lockable

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

lockable

no lockable

Parameter description

None

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:

```
DGS-3610(config)# line console 0
DGS-3610(config-line)# lockable
DGS-3610(config-line)# end
DGS-3610# lock
Password: <password>
Again: <password>
Locked
```

```
Password: <password>
DGS-3610#
```

Related commands

Command	Description
lock	Lock the terminal.

2.1.12 telnet

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

telnet *host* [*port*] [*keyword*]

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.
Keyword	The available keywords are listed in the table below:

Keyword	Description
/source-interface	Specify the interface from which the telnet connection request is sent.
/vrf	Specify the queried VRF routing table.

Command mode

Privileged mode.

Usage guidelines

This command is used to log in a telnet server.

Caution

/vrf keyword, which is only applicable to the RSR system router!

Examples

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

```
DGS-3610# telnet 192.168.1.11 /soource-interface vlan 1 /vrf
vpn1
```

Related

Command	Description

commands	**Show session**	View the session established by current TTY.
	Exit	Exit current connection.

2.1.13 enable service

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

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

Parameter description	**Keyword**	**Description**
	ssh-sesrver	Enable and disable SSH Server
	telnet-server	Enable and disable Telnet Server
	web-server	Enable and disable Http Server
	snmp-agent	Enable and disable Snmp Agent

Command mode	Global configuration mode
Usage guidelines	This command is used to enable or disable the specified service. Use **no enable service** command to disable the specified service.
Examples	Following Example: **Enable the SSH Server,** Enable the function of SSH Server: DGS-3610(Config)# **enable service ssh-sesrver**

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

2.2 Basic System Management Related Commands

The system management includes related commands as follows:

- **clock set**
- **hostname**
- **show clock**
- **show running-config**
- **show startup-config**
- **reload**

- **show reload**
- **prompt**
- **banner motd**
- **banner login**
- **speed**
- **show line**
- **write**

2.2.1 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

This command is used to set the system time to facilitate the management.

For devices without hardware clock, the time of the device set by clock set is effective for only the current setting. When the device powers off, the manually set time is lost.

These devices have not hardware clock: S2026G, S2026F, S2028, and RSR10.

Examples

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

```
DGS-3610# clock set 10:20:30 Mar 17 2003
DGS-3610# show clock
clock: 2003-3-17 10:20:32
```

Related

Command	Description

commands	**show clock**	Show current clock

2.2.2 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“.

```
DGS-3610(config-line)#exec-timeout 5 30
```

2.2.3 hostname

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

hostname *name*

Parameter description

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

Default configuration	The default hostname is DGS-361.
Command mode	Global Configuration Mode
Usage guidelines	This hostname is mainly used to identify the router and is taken as the username for the local router in the dialup and CHAP authentication.

Examples	The example below configures the hostname of the router as BeiJingAgenda:
	`DGS-3610(config)# hostname D-Link`
	`D-Link(config)#`

2.2.4 session-timeout

To configure the session timeout for the remote terminal established in current LINE, use the **session-timeout** command. Execute the **no session timeout** for cancelling the session timeout of the remote terminal in the LINE, the session will never be timeout.

session-timeout *minutes [seconds]*

no session-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 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 min plus 30

second.

```
DGS-3610(config-line)# exec-timeout 5  30
```

2.2.5 show clock

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

show clock [**detail**]

Parameter description

Parameter	Description
detail	Show the source of system clock.

Command mode

Privileged mode.

Usage guidelines

This command is used to view current system clock, the **detail** option will show the source of the system clock.

Examples

The example below is an execution result of the **show clock** command:

```
DGS-3610# show clock detail
clock: 2003-3-17 10:27:21
Clock read from calendar when system boot.
```

Related commands

Command	Description
clock set	Set the system clock.

2.2.6 show running-config

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

show running-config

Command mode

Privileged mode.

2.2.7 show startup-config

To view the configuration of router 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 router stored in the NVRAM is that executed when the router is started.

2.2.8 reload

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

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

Parameter description

Parameter	Description
text	Cause for restart, 1-255 bytes
in *[hh:] mm*	The system is restarted after specified time interval, and the maximum interval is 24 days.
at *hh:mm*	The system is restarted at the specified time.
month	The indication of Month in the character, such as Mar for March
day	Date, 1~31
cancel	Cancel scheduled restart.

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

Examples	The example below specifies to restart the system in 10 minutes:
	`DGS-3610# reload in 10`
	`Router will reload in 600 seconds.`

2.2.9 show reload

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

show reload

Parameter description	None

Command mode	Privileged mode.
Usage guidelines	Use this command to show the restart settings of the system.

Examples	Following example to show the restart settings of the system:
	`DGS-3610# show reload`
	`Reload scheduled in 595 seconds.`
	`At 2003-12-29 11:37:42`
	`Reload reason: test.`

2.2.10 prompt

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

prompt *string*

Parameter description

Parameter	Description
string	Character string of the command prompt. 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 command prompt is valid in only the EXEC mode.

Examples	Set the prompt string to DGS-3610:
	`DGS-3610(config)# prompt D-Link`
	`DGS-3610(config)# end`
	`D-Link`

2.2.11 banner motd

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

banner motd *c message c*

Parameter description

Parameter	Description
c	Separator of the MOTD. Delimiters are not allowed in the MOTD.
message	Configure an MOTD Login Banner

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:

```
DGS-3610(config)
DGS-3610(config)# banner motd $ hello,world $
```

2.2.12 banner login

To configure the banner login, please execute the command **banner login** in the global configuration mode. You can use **no banner login** command to delete the configuration of logging banner.

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	Configure the message of logging 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:

```
DGS-3610(config)
DGS-3610(config)# banner login $ enter your password $
```

2.2.13 speed

To set the terminal rate, run **speed** in the line configuration mode. To reset the terminal speed to its default value, run **no speed**.

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. The default rate is 9600 bps.

Command mode

Global configuration mode

Default Configuration

The default rate is 9600.

Usage guidelines

This command sets the terminal rate.

Examples

The following example shows how to configure the rate of the serial port to 57600 bps:

```
DGS-3610(config)#
DGS-3610(config)# line console 0
DGS-3610(config-line)# speed 57600
DGS-3610(config-line)#
```

2.2.14 show line

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

show line [**console** *line-num* **| aux** *line-num* **| vty** *line-num* **|** *line-num*]

Parameter description

Parameter	Description
console	Show the configuration of console line
aux	Show the configuration of aux line
vty	Show the configuration of vty line
line-num	show the line

Command mode	Privileged mode.
Default Configuration	
Usage guidelines	This command shows the configuration information of each line.

Examples	Following example shows the configuration of console port:
	`DGS-3610# 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`

2.2.15 write

To perform the read/write operation for the router 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 to 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. This command without an option is equivalent to the command with the **memory** option.

Examples	The example below saves the router configuration:
	`DGS-3610# write`
	`Building configuration...`
	`[OK]`

Related commands

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

3 Configuring LINE Command

3.1 Configuration Related Commands

3.1.1 line

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

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

Parameter description

Parameter	Description
First-line	Number of first-line to enter
Last-line	Number of last-line to enter

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

Enter the specified LINE mode

Examples

Enter the LINE mode from LINE VTY 1 to 3:

```
DGS-3610(config)# line vty 1 3
```

Related commands

None

3.1.2 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.
	`DGS-3610(config)# line vty 19`
	Decrease the number of available VTY connections to 10. The available VTY connections are numbered 0-9.
	`DGS-3610(config)# line vty 10`

Related commands	None

3.1.3 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:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# line vty 0 4`
	`DGS-3610(config-line)# transport input telnet`

Related commands

Command	Description
show running	Show status information

Version description	The software version must be later than v10.1.

3.1.4 access-class

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

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

Parameter description

Parameter	Description
access-list-number	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:

```
DGS-3610# configure terminal
DGS-3610(config)# line vty 0 4
DGS-3610(config-line)# access-class 10 in
```

Related commands

Command	Description
show running	Show status information

Version description

The software version must be later than v10.1.

4 Configuring Upgrade and Maintenance Commands of the System

4.1 Configuration Related Commands

The following describes how to upgrade and maintain by using the COPY command in the CLI environment of the main program.

- Upgrade and maintain by Xmodem protocol: **copy xmodem** command.
- Upgrade and maintain by Tftp protocol: **copy tftp** command.

4.1.1 copy xmodem

Upgrade and maintain by using the xmodem protocol or upload and download by using the xmodem protocol.

copy flash: *filename* **xmodem**

copy xmodem flash: *filename*

Parameter description

Parameter	Description
filename	The name of files in the equipment.

Default

No default value

Command mode

Privileged mode.

Usage guidelines

If the file is transmitted successfully, show the length of the transmitted file; otherwise, show the failure information. Any files can be transmitted by TFTP, such as main program file and parameter file. The Xmodem can only be transmitted in the out-band (serial ports).

The following shows two examples: The first one transmits the files to the switch from the host via the xmodem protocol. The second

	uploads the configuration file in the switch to the host via the xmodem protocol.

Examples	The following is an example of upload and download:
	`DGS-3610# copy xmodem flash: config.text`
	`DGS-3610# copy flash: config.text xmodem`

Related commands	No related command.

4.1.2 copy tftp

Upgrade and maintain by the tftp protocol or upload and download by the tftp protocol.

copy flash: *filename* **tftp**:///*location/filename*

copy tftp:///*location/filename* **flash**: *filename*

Parameter description

Parameter	Description
filename	The name of files in the equipment.

Default	No default value.
Command mode	Privileged user mode.
Usage guidelines	If the file is transmitted successfully, show the length of the transmitted file. Otherwise, show the failure information. Any files can be transmitted by TFTP, such as main program file and parameter file. The TFTP transmission is carried out by the network port.

Examples	The following is two examples: The first one transmits the backup parameter file (config.bak) from the local host (ip 192.168.12. 1) to the switch; The second one transmits the file (switch.bin) from the switch to the local switch (ip 192.168.12.1):
	`DGS-3610# copy tftp://192.168.12.1/confg.bak flash: config.text`
	`DGS-3610# copy flash: swhich.bin tftp://192.168.12.1/`

Related commands	No related command.

5 Configuring Network Connectivity Test Tool Configuration Commands

5.1 Configuration Related Commands

The network connectivity test tool configuration commands include:

- **ping**
- **traceroute**

5.1.1 ping

This command is used to test the connectivity of a network for the user to diagnose and locate the network connectivity problem. The command format is as follows:

ping [**vrf**] [*vrf-name*] [**ip**] [*ip-address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*]]

Parameter description

Parameter	Description
ip-address	Specify an IPv4 address.
length	Specify the length of the packet to be sent.
times	Specify the number of packets to be sent.
timeout	Specify the timeout time.
vrf-name	VRF name

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 100 bytes 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, '.' Is 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. The VRF function is provided in the RSR equipment only.

Examples

The example below shows the ordinary ping.

```
DGS-3610# 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.

```
DGS-3610# ping 192.168.5.197 length 1500 ntimes 100 timeout 3
Sending 100, 1000-byte ICMP Echoes to 192.168.5.197, 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
DGS-3610#
```

Platform description

The command is supported by all devices.

5.1.2 Traceroute

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

traceroute [**ip** *ip-address*][*ip-adress*]

Parameter description

Parameter	Description
ip-address	Specify an IPv4 address.
vrf-name	VRF name

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. The VRF function can only be provided in the RSR device.

Examples

The following is two examples of the application about traceroute, the one is of the smooth network, and the other is the network in which some gateways are not connected successfully.

1. When the network is connected smoothly:

```
DGS-3610# 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
DGS-3610#
```

The gateways that the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) pass through and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways fail in the network :

```
DGS-3610# 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
DGS-3610#
```

The gateways that the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) pass through and the spent time are displayed, and gateway 4 fails.

```
DGS-3610# traceroute www.dlink.com.tw

Translating "www.dlink.com.tw"...[OK]
  < press Ctrl+C to break >
Tracing the route to 61.233.3.212

 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    61.233.3.212   40 msec 40 msec 40 msec
```

Platform description

The command is supported by all devices. The VRF function can only be provided in the RSR device.

6 Configuring Interface Commands

6.1 Configuration Related Commands

Interface configuration includes the following commands:

- **interface aggregateport**
- **interface fastEthernet**
- **interface giagbitEthernet**
- **interface tenGigabitEthernet**
- **interface vlan**
- **medium-type**
- **descriptioin**
- **shutdown**
- **speed**
- **duplex**
- **flowcontrol**
- **mtu**
- **clear counters**
- **clear interface**
- **switchport**

6.1.1 interface aggregateport

This command is a mode navigation command that is used to create or access or create the Aggregate port, and enter to the interface configuration mode. Use the **no** form of the command to remove this interface.

interface aggregateport *port-number*

	Parameter	Description
Parameter description	*port-number*	Aggregate port number, with its range determined by the equipment and extended

	module

Command mode

Global configuration mode.

Usage guidelines

According to some rules, you can add physical ports to an aggregate port. The attributes of all the member ports in the aggregate port is specified by the aggregate port. You can use **show interfaces** or **show interfaces aggregateport** commands to display the interface configuration.

Examples

```
DGS-3610(config)#interface aggregateport 3
DGS-3610(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.2 interface fastEthernet

This command is a mode navigation command that is used to select a Fast Ethernet interface and enter interface configuration.

interface fastEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	The module number/the port number on the module. 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 configuration.

Examples

```
DGS-3610(config)# interface fastEthernet 1/2
DGS-3610(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.3 interface giagbitEthernet

This command is a mode navigation command that is used 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 module number/the port number on the module. 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

```
DGS-3610(config)# interface gigabitEthernet 1/2
DGS-3610(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.4 interface tenGigabitEthernet

This command is a mode navigation command that is used to select 10G Ethernet interface, and the enter interface configuration mode.

interface tenGigabitEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	Module number/port number on the module. 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	`DGS-3610(config)# interface tenGigabitEthernet 1/2` `DGS-3610(config-if)#`

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description	Currently, no product supports this command.

6.1.5 interface vlan

This command is a mode navigation command that is used to create or access a dynamic switch virtual interfact (SVI), and enter the interface configuration mode. 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, the range is defined by the device.

Command mode	Global configuration mode.
Usage guidelines	Use **show interfaces** or **show interfaces vlan** to display the interface configurations.
Examples	`DGS-3610(config)# interface vlan 2` `DGS-3610(config-if)#`

Related

Command	Description

commands	**show interfaces**	Show the interface settings and static information.

6.1.6 medium-type

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

medium-type { **fiber | copper** }

no medium-type

Parameter description

Parameter	Description
fiber	Means to select a fiber interface.
copper	Means to select a copper interface.

Default configuration

The default value is copper interface.

Command mode

Interface configuration mode (physical interface, except AP and SVI)

Usage guidelines

If a port can be selected as an optical port or copperl 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 reconfigured as needed.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# medium-type copper
```

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description

The 12 SFP interfaces of the 24SFP/12GT line cards and twelve 10/100/1000M BASE-T interfaces allow dynamic switching.

The duplicate interface is not supported to automatically distinguish the current working port, whether the SFP interface or the 10/100/1000M BASE-T interface.

6.1.7 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	The 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

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# description GBIC-1
```

Related commands

Command	Description
show interfaces	Show the interface settings and static information.

6.1.8 shutdown

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

shutdown

no shutdown

Command mode

Interface configuration mode.

Usage guidelines

For the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can disaable the interfaces with this command, .the other configuration of the interfaces still exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

Examples

Disable Ap 1**:**

```
DGS-3610(config)# interface aggregateport 1
DGS-3610(config-if)# shutdown
```

Enable Ap 1**:**

```
DGS-3610(config)# interface aggregateport 1
DGS-3610(config-if)# no shutdown
```

Related commands

Command	Description
clear interface	Reset the the interface hardware.
show interfaces	Show the interface settings and statistic information.

Note

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

6.1.9 speed

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

Parameter description

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

Default configuration	It's auto-adaptive by default.
Command mode	Interface configuration mode
Usage guidelines	If an interface is the member of the Ap, the rate of the interface depends on the rate of the Ap. You can still set the rate of the interface, but it does not take effect. After the interface exits the Ap, it uses its own rate. Use **show interfaces** to display configuration. Different types of interfaces allow different types of rates to be set. For example, a SFP interface does not allow you to set the rate to 10M or 100M.
Examples	`DGS-3610(config)# interface gigabitethernet 1/1` `DGS-3610(config-if)# speed 100`

Related commands

Command	Description
show interfaces	Show the interface settings and statistic information.

6.1.10 duplex

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

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

no duplex

Parameter description

Parameter	Description
auto	Means the auto-adaptive in full- or half-duplex mode.
full	Means that the interfae is in full-duplex mode.
half	Means that the interfae is in half-duplex mode.

Default configuration	The default is the auto-adaptive in full- or half-duplex mode.

Command mode

Interface configuration mode.

Usage guidelines

The duplex attribute of the interface is associated with the interface type. Use **show interfaces** to display the duplex configuration of the interface.

Examples

```
DGS-3610(config-if)# duplex full
```

Related commands

Command	Description
show interfaces	Show the interface settings and statistic information.

6.1.11 flowcontrol

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

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

no flowcontrol

Parameter description

Parameter	Description
auto	Auto-negotiation the flow control.
off	Disable the flow control.
on	Enable the 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 of the interface and actual flow control.

Examples

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

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# flowcontrol on
```

Related commands

Command	Description
show interfaces	Show the interface settings and statistic information.

6.1.12 mtu

Set a MTU supported by the interface

Mtu *num*

Parameter description

Parameter	Description
num	The ranged is from 64 to 9216 (or 65536. It's vary depending on the different product).

Default configuration

By default, the value is 1500.

Command mode

Interface configuration mode.

Usage guidelines

Set a MTU (Maximum Transmission Unit) supported by the interface. Currently, this device only support setting of a physical interface.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# mtu 9216
```

Related commands

Command	Description
show interfaces	View interface setting and statistics.

6.1.13 carrier-delay

In the interface configuration mode, you can use the **carrier-delay** command to set the carrier delay of the interface, and the **no** form of this command to restore the default value.

carrier-delay [*seconds*]

no carrier-delay

Parameter description

Parameter	Description
seconds	Optional parameter, in seconds, within the

		range of 1~60 seconds

Default configuration

The default carrier delay is 2 seconds.

Command mode

Interface configuration mode.

Usage guidelines

This parameter is 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 is changed 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 convergence so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is smaller than the time for route convergence, 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 as 5 seconds:

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(coinfig)# carrier-delay 5
```

6.1.14 clear counters

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

clear counters [*interface-id*]

Parameter description

Parameter	Description
interface-id	The interface type and interface ID.

Command mode

Privileged mode.

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

Examples

```
DGS-3610# clear counters gigabitethernet 1/1
```

Related commands

Command	Description
show interfaces	Show the interface settings and statistic information.

6.1.15 clear interface

Reset interface hardware.

clear interface *interface-id*

Parameter description

Parameter	Description
interface-id	The interface type and interface ID.

Command mode

Privileged mode.

Usage guidelines

This command is only used on Switch Port, member port of the L2 Aggregate port, member port of the Routed port, and L3 Aggregate port. This command is equal to the **shutdown** and **no shutdown** command.

Examples

```
DGS-3610# clear interface gigabitethernet 1/1
```

Related commands

Command	Description
shutdown	Shutdown the interface.

6.1.16 switchport

In 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 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 prodedure, 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	`DGS-3610(config-if)# switchport`

Related commands

Command	Description
show interfaces	Show the interface settings and statistic information.

6.1.17 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 a 802.1Q tunnel. Use the **no** form of the command to restore the default setting.

switchport mode {**access | trunk**}

no switchport mode

Parameter description

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

Default configuration	The default mode of switch port is access.
Command mode	Interface configuration mode.

Usage guidelines

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

If the mode of a swotch port is trunk, this interface can be the member port of multiple VLANs. 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 of the interface.

Examples

```
DGS-3610(config-if)# switchport mode trunk
```

Related commands

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

6.1.18 switchport access

Use this command to configure an interface as access port and assign it to a VLAN member port. 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	ID of the VLAN to which the port is to be added.

Default configuration

The default mode of switch port is access, and the default VLAN is VLAN 1

Command mode

Interface configuration mode.

Usage guidelines

Enter one VLAN ID. If a new VLAN ID is entered, a VLAN will be created and the port is set as a member of the VLAN. If the VLAN ID already exists, the command adds the member port of the VLAN.

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

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(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.

6.1.19 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport. 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. Parameter vlan-list can be a VLAN or a range of VLANs described by VLAN IDs, the lower one first, and the bigger one end, separated by hyphen(-). For example: 10-20. The segments can be separated with a comma (,), for example, 1-10, 20-25, 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*	Configure the native VLAN.

Default configuration

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

Command mode

Interface configuration mode.

Usage guidelines

Native VLAN:
As the trunk, the port belongs to one native VLAN. A native VLAN means that the UNTAG packets received/sent at the interface are deemed as belonging 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, the UNTAG mode is bound to be used.
Allowed-VLAN List:
By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1-4094). 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 VLAN 2 from port 1/15:

```
DGS-3610(config)# interface fastethernet 1/15
DGS-3610(config-if)# switchport trunk allowed vlan remove 2
DGS-3610(config-if)# end
DGS-3610# show interfaces fastethernet1/15 switchport
Switchport is enabled
Mode is trunk port
Acsess 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 statics accessport and assign it to a VLAN.

6.1.20 snmp trap link-status

You can set whether to send the interface-based LinkTrap of this interface. If the function is enabled, the SNMP sends the LinkTrap when the Link status of the interface changes. The **no** form of this command prevents the SNMP 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 Ethernet port, Ap port, and SVI port, this command sets whether to send the interface-based LinkTrap. If the function is enabled, the SNMP sends the LinkTrap when the Link status of the port changes.

Examples	Disable the sending of Link trap:
	`DGS-3610(config)# interface gigabitEthernet 1/1`
	`DGS-3610(config-if)# no snmp trap link-status`
	Following configuration shows how to configure the interface to forwarding Link trap:
	`DGS-3610(config)# interface gigabitEthernet 1/1`
	`DGS-3610(config-if)# snmp trap link-status`

Related commands

Command	Function
DGS-3610(config-if)# **snmp trap link-status**	Function of enabling the forwarding link trap of this interface.
DGS-3610(config-if)# **no snmp trap link-status**	Function of disabling the forwarding interface link trap.

6.2 Showing Related Command

6.2.1 show interfaces

Show the interface information.

show interfaces [*interface-id*] [**counters | description | status | switchport | trunk**]

Parameter description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregateport, or SVI and loopback interface).
counters	The statistic information 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 transmission rate and duplex.
switchport	Layer 2 interface information, only applicable for L2 interface..
trunk	Information about the trunking port, applicable for physical port and Aggregate port

Default configuration

Show all the interface information.

Command mode

Privileged mode.

Usage guidelines

Show the basic information of the interface if not specify the parameters.

Related commands

Command	Description
duplex	Perform the Duplex settings of the interface.
flowcontrol	Enable or disable the flow control.
interface gigabitEthernet	Select the Ethernet interface (including gigabitEthernet interface), and enter interface configuration mode.
interface aggregateport	Create or access the aggregateport, and enter interface configuration mode.
interface vlan	Create or access a dynamic switch virtual interface (SVI), and enter interface configuration mode.
shutdown	Use the command to disable an interface in the interface configuration mode.
speed	Use this command to configure the speed on the intef
switchport priority	Use this command to configure the default interface priority for 802.1q .
switchport protected	Set the interface as protected port.

7 Configuring Aggregate Port Command

7.1 Configuration Related Commands

7.1.1 port-group

Use this command to configure a physical interface as the member port of the Aggregate Port. Use the **no** form of the command to delete the membership attribute from the aggregate port.

port-group *port-group-number*

no port-group

Default configuration

By default, the physical port does not belong to any Aggregate Port.

Parameter description

Parameter	Description
port-group-number	Group number of the Aggregate Port member port. Namely the interface number of the Aggregate Port.

Command mode

Interface configuration mode.

Usage guidelines

Include all the AP member interfaces in one VLAN or configure all of them as trunk ports. The interfaces belongings to different native VLANs can not consist the AP.

Examples

This example shows how to specify the Ethernet interface 1/3 and 1/4 as members of AP 3:

```
DGS-3610(config)# interface gigabitethernet 1/3
DGS-3610(config-if)# port-group 3
```

7.1.2 aggregateport load-balance

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

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

dst-ip | **src-ip** | **ip** }

no aggregateport load-balance

Parameter description

Parameter	Description
dst-mac	Traffic is distributed according to the source MAC addresses of the incoming packets. In all the links of the AP, the messages with the same destination MAC addresses are sent to the same interface, and those with different destination MAC addresses are sent to different interfaces.
src-mac	Traffic is distributed according to the source MAC addresses of the inputting packets. In all the links of the AP, the messages from different addresses are distributed to different interfaces, and those from the same addresses are distributed to the same interface.
ip	Traffic is distributed according to the source IP and destination IP. Packets with different source-destination IP address pairs are forwarded through different ports. The packets with the same source-destination MAC address pairs are forwarded through the same links. At layer 3, this traffic balancing style is recommended.
dst-ip	Traffic is distributed according to the source MAC addresses of the incoming packets. In all the links of the AP, the messages with the same destination MAC addresses are sent to the same interface, and those with different destination MAC addresses are sent to different interfaces.
src-ip	Traffic is distributed according to the source MAC addresses of the incoming packets. In all the links of the AP, the messages from different addresses are distributed to different interfaces, and those from the same addresses are distributed to the same interface.
src-dst-mac	Traffic is distributed according to the source IP and destination IP. Packets with different source-

		destination IP address pairs are forwarded through different ports. The packets with the same source-destination MAC address pairs are forwarded through the same links.

Default configuration	Traffic is distributed according to the destination and source MAC addresses of the inputting packets
Command mode	Global configuration mode.
Usage guidelines	Use **show aggregateport load-balance** to display traffic balance algorithm.
Examples	`DGS-3610(config)# aggregateport load-balance dst-mac`

Related commands

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

7.2 Showing Related Command

7.2.1 show aggregateport

Use this command to display aggregateport configurations.

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

load-balance}

Parameter description

Parameter	Description
aggregate-port-number	Interface number of Aggregate Port.
load-balance	Show aggregate port traffic balance algorithm.
summary	Show the summary of each link on the aggregate port ..

Command mode

Privileged mode.

Usage guidelines

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

Examples

```
DGS-3610# show aggregateport 1 summary
AggregatePort  MaxPorts       SwitchPort Mode   Ports
-------------  --------       -------------   ------
Ag1              8             Enabled     ACCESS
```

Related commands

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

8 Configuring VLAN Command

8.1 Configuration Related Commands

8.1.1 vlan

This command is a mode navigation command that is used to enter 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 Note: Default VLAN (VLAN 1) shall not be removed.

Command mode

Global configuration mode.

Usage guidelines

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

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

Examples

```
DGS-3610(config)# vlan 1
DGS-3610(config-vlan)#
```

Related commands

Command	Description
show vlan	Show member ports on the VLAN.

8.1.2 name

Set the VLAN name. Use the **no** form of the command to restore the default setting.

name *vlan-name*

no name

Parameter description

Parameter	Description
vlan-name	The name of VLAN..

Default configuration

There is no name of VLAN by default.

Command mode

VLAN configuration Mode.

Usage guidelines

You can view the vlan settings by using the **show vlan** command.

Examples

```
DGS-3610(config)# vlan 10
DGS-3610(config-vlan)# name vlan10
```

Related commands

Command	Description
show vlan	Show member ports on the VLAN.

8.1.3 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 a 802.1Q tunnel. Use the **no** form of the command to restore the default setting.

switchport mode {**access** | **trunk**}

no switchport mode

Parameter description

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

Default configuration

The default mode of switch port is access.

Command mode

Interface configuration mode.

Usage guidelines	If a switch port mode is access, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN. 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	`DGS-3610(config-if)# switchport mode trunk`

Related commands

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

8.1.4 switchport access

Use this command to configure an interface as access port and assign it to a VLAN member port. 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	VLAN ID to be added on the port.

Default configuration	The default mode of switch port is Access, and the default VLAN is VLAN 1
Command mode	Interface configuration mode.
Usage guidelines	Enter one VLAN ID. If a new VLAN ID is entered, a VLAN will be created and the port is set as a member of the VLAN. If the VLAN ID already existed, the command adds the member port of the VLAN. If the port is a trunkport, the operation does not take effect.
Examples	`DGS-3610(config)# interface gigabitethernet 1/1` `DGS-3610(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.

8.1.5 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport. 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. Parameter vlan-list can be a VLAN or a range of VLANs described by VLAN IDs, the lower one first, the higher one end, separated by a hyphen (-). For example: 10-20. The segments can be separated with a comma (,), for example, 1-10, 20-25, 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*	Configure the Native VLAN.

Default configuration

The configuration of default allowed-VLAN list is all, and the default native VLAN is VLAN 1.

Command mode

Interface configuration mode.

Usage guidelines

Native VLAN:

As the Trunk, the port belongs to one native VLAN. A native VLAN means that the UNTAG packets received/sent at the interface are deemed as belonging 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, the UNTAG mode is bound to be used.

Allowed-VLAN List:

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

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

Examples

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

```
DGS-3610(config)# interface fastethernet 1/15
DGS-3610(config-if)# switchport trunk allowed vlan remove 2
DGS-3610(config-if)# end
DGS-3610# show interfaces fastethernet1/15 switchport
Switchport is enabled
Mode is trunk port
Acsess 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 statics accessport and assign it to a member port of VLAN.

8.2 Showing Related Command

8.2.1 show vlan

Show member ports on the VLAN.

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

Parameter description

Parameter	Description
vlan-id	VLAN ID

Default configuration

All the information is shown by default.

Command mode

Privileged mode.

Usage guidelines

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

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

Examples

```
DGS-3610# show vlan id 1
VLAN[1] "VLAN0001"
       GigabitEthernet 3/1
       GigabitEthernet 3/2
       GigabitEthernet 3/3
       GigabitEthernet 3/4
       GigabitEthernet 3/5
       GigabitEthernet 3/6
       GigabitEthernet 3/7
       GigabitEthernet 3/8
       GigabitEthernet 3/9
       GigabitEthernet 3/10
       GigabitEthernet 3/11
       GigabitEthernet 3/12
```

Related commands

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

9 Configuring Supervlan Command

9.1 Configuring Related Commands

9.1.1 supervlan

Use this command to set the VLAN as **supervlan**.

supervlan

no supervlan

Parameter description	No parameters.
Command mode	VLAN configuration Mode.
Usage guidelines	To return to privileged mode, input **end** or press **Ctrl+C**. To return to global configuration mode, input **exit.**
Examples	`DGS-3610(config)# vlan 3` `DGS-3610(config-vlan)# supervlan`

Related commands

Command	Description
show supervlan	Show the supervlan information.

Platform description	None.

9.1.2 subvlan

Use this command to set the subvlan of this super vlan or delete subvlan.

subvlan *vlan-id-list*

no subvlan *[vlan-id-list]*

Parameter description

Parameter	Description
Vlan-id-list	The subvlan ID of this VLAN supports several vlan at the same time.

Command mode

VLAN configuration mode.

Usage guidelines

Use **no subvlan** command to delete all subvlan of this supevlan.

Examples

```
DGS-3610(config)# vlan 3
DGS-3610(config-vlan)# supervlan
DGS-3610(config-vlan)# subvlan 5
DGS-3610(config-vlan)# subvlan 7-19
```

Related commands

Command	Description
show supervlan	Show the supervlan information.

Platform description

9.1.3 subvlan-address-range

Use this command to set the ip address range of the subvlan.

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

no subvlan-address-range

Parameter description

Parameter	Description
start-ip	The start IP address of this SubVLAN
end-ip	The end IP address of this SubVLAN

Command mode

VLAN configuration mode.

Usage guidelines

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

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

Examples

```
DGS-3610(config)# vlan 3
DGS-3610(config-vlan)# subvlan-address-range
192.168.3.10 192.168.3.100
```

Related commands

Command	Description
show supervlan	Show the supervlan information.

Platform description

None.

9.1.4 proxy-arp

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

proxy -arp

no proxy -arp

Parameter description

No parameters.

Command mode

VLAN configuration mode.

Usage guidelines

To return to privileged mode, input **end** or press **Ctrl+C**.
To return to global configuration mode, input **exit.**

Examples

```
DGS-3610(config)# vlan 3
DGS-3610(config-vlan)# agent-arp
```

Related commands

Command	Description
show supervlan	Show the supervlan information.

Platform description

None.

9.2 Showing Related Command

9.2.1 show supervlan

Use this command to show the configuration of SuperVLAN and SubVLAN.

show supervlan

show supervlan id *vlan-id*

Parameter description

Parameter	Description
vlan-id	The ID of this VLAN

Command mode

Privileged mode.

Usage guidelines

None.

Examples

```
DGS-3610# show supervlan
supervlan id  supervlan arp-agent  subvlan id  subvlan arp-agent
subvlan ip range
-------   ----------  -------------   -----------------
3               ON          4               ON
                            5               ON
```

Related commands

None

Platform description

None

10 Configuring Protocol VLAN Commands

10.1 Configuration Related Commands

- **protocol-vlan ipv4** *addr* **mask** *addr* **vlan** *id*
- **protocol-vlan profile** *num* **frame-type** *[type]* **ether-type** *[type]*
- **protocol-vlan profile** *num* **vlan** *id*

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

Configure the IP address, subnet mask and VLAN classification.

Parameter description

Parameter	Description
addr	IP address, input it in the x.x.x.x format.
id	VLAN ID, the maximal VLAN supported by the product 1.

Default configuration

None.

Command mode

Global configuration mode.

Examples

```
DGS-3610(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 later than v10.1.

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

Configure the **profile** of the message type and profile of the Ethernet type.

Parameter description

Parameter	Description
num	Profile indexes
type	The type of message and that of Ethernet

Default configuration	None.
Command mode	Global configuration mode.
Examples	`DGS-3610(config)# protocol-vlan profile 1 frame-type ETHERII ether-type EHTER_aarp`
Related commands	**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 later than v10.0.

10.1.3 protocol-vlan profile *num* vlan *id*

Apply a profile to this interface.

Parameter description

Parameter	Description
num	profile indexes
id	VLAN ID, the maximal VLAN the product 1 supported.

Command mode	Interface mode.
Examples	`DGS-3610(config-if)# protocol-vlan profile 1 vlan 101`
Related commands	**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 later than v10.1.

10.2 Show Commands

- **show protocol-vlan**

10.2.1 show protocol-vlan

Show the configuration of Protocol VLAN.

show vlan protocol-vlan

Parameter description	None.
Default configuration	None.
Command mode	Privileged mode.
Examples	`DGS-3610# show protocol-vlan`
Platform description	The software version must be later than v10.1.

11 Configuring Private VLAN Command

11.1 Configuration Related Commands

- **private-vlan type**
- **private-vlan association**
- **private-vlan mapping**
- **switchport mode private-vlan**
- **switchport private-vlan host-association**
- **switchport private-vlan mapping**

11.1.1 private-vlan *type*

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 a community VLAN.
isolated	Configure it as an isolated VLAN.
primary	Configure it as a primary VLAN.
no	Delete corresponding private VLAN configuration.

Default configuration

No private VLAN.

Command mode

VLAN configuration Mode

Examples

```
DGS-3610(config)# vlan 22
DGS-3610(config-vlan)# private-vlan primary
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be later than v10.1.

11.1.2 private-vlan association

Associate the secondary VLAN configuration command with the primary VLAN to configuration command.

private-vlan association {*svlist* **| add** *svlist* **| remove** *svlist*}

no private-vlan association

Parameter description

Parameter	Description
svlist	The secondary VLAN list.
no	Cancel the association of primary VLAN with all secondary VLANs.

Default configuration

No association.

Command mode

VLAN configuration Mode.

Examples

```
DGS-3610(config)# vlan 22
DGS-3610(config-vlan)# private-vlan association add 24-26
```

Related commands

show vlan private-vlan

Platform description

The software version must be later than v10.1.

11.1.3 private-vlan mapping

Map the secondary VLAN to L3 SVI interface command.

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

```
DGS-3610(config)# interface vlan 22
DGS-3610(config-if)# private-vlan mapping add 24-26
```

Related commands

show vlan private-vlan

Platform description

The software version must be later than v10.1.

11.1.4 switchport mode private-vlan

Declare that the interface is in the private VLAN mode.

switchport mode private-vlan{**host|promiscuous**}

no switchport mode

Parameter description

Parameter	Description
host	The host mode of private VLAN
promiscuous	The hybrid mode of private VLAN
no	Delete the private VLAN configuration of the port.

Command mode

Interface mode.

Examples

```
DGS-3610(config)# interface gigabitEthernet0/2
DGS-3610(config-if)# switchport mode private-vlan host
```

Related commands	**show vlan private-vlan**

Platform description	The software version must be later than v10.1.

11.1.5 switchport private-vlan host-association

Associate the primary VLAN mode, which is associated with the private VLAN mode host 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	Created primary VID
s_vid	Created secondary VID
no	Delete the host port from the private VLAN.

Command mode	Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# switchport mode private-vlan host
DGS-3610(config-if)# switchport private-vlan host-association 22
23
```

Related commands	**show vlan private-vlan**

Platform description	The software version must be later than v10.1.

11.1.6 switchport private-vlan mapping

The hybrid interface of the private VLAN configures required hybrid secondary VLAN.

switchport private-vlan mapping *p_vid* {*svlist*|**add** *svist* |**remove** *svlist*}

no switchport private-vlan mapping

Parameter description

Parameter	Description
p_vid	Created primary VID.
svlist	Created secondary VLAN list.
no	Cancel all hybrid secondary VLANs.

Default configuration

No hybrid secondary VLAN.

Command mode

Hybrid interface of private VLAN.

Examples

```
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# switchport mode private-vlan promiscuous
DGS-3610(config-if)# switchport private-vlan mapping 22 add 23-25
```

Related commands

show vlan private-vlan

Platform description

The software version must be later than v10.1.

11.2 Showing Commands

- **show vlan private-vlan**

11.2.1 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.

Command mode Privileged mode.

Examples

```
DGS-3610# show vlan private-vlan
```

Platform description The software version must be later than v10.1.

11.3 Hybrid Commands

- **switchport mode hybrid**
- **switchport hybrid native vlan**
- **switchport hybrid allowed vlan**

11.3.1 switchport mode hybrid

switchport mode hybrid

no switchport mode

Configure the port as hybrid port.

Parameter description

Parameter	Description
no	Delete the hybrid mode.

Default configuration None.

Command mode Interface configuration mode.

Examples

```
DGS-3610(config-if)# switchport mode hybrid
```

Platform description The software version must be later than v10.1.

11.3.2 switchport hybrid native vlan

switchport hybrid native vlan *vid*

no switchport hybrid native vlan

Configure the default vlan of hybrid port.

Parameter description

Parameter	Description
no	Restore the hybrid to default VLAN.

Default configuration None.

Command mode Interface mode.

Examples DGS-3610(config-if)# **switchport hybrid native vlan** *3*

Platform description The software version must be later than v10.1.

11.3.3 switchport hybrid allowed vlan

switchport hybrid allowed vlan[[add][tagged | untagged] | remove] v*list*

no switchport hybrid allowed vlan

Configure the output rules of hybrid port.

Parameter description

Parameter	Description
no	Restore the default output rules of the hybrid.

Default configuration None.

Command mode Interface configuration mode.

Examples

```
DGS-3610(config-if)# switchport hybrid allowed vlan add untagged
3-5
```

Platform description The software version must be later than v10.1.

12 Configuring 802.1Q Tunneling Commands

12.1 Configuration Related Commands

- **switchport mode dot1q-tunnel**
- **switchport mode uplink**
- **frame-tag tpid** *tpid*
- **inner-priority-trust enable**

12.1.1 switchport mode dot1q-tunnel

Configure the interface as the 802.1Q tunneling interface.

switchport mode dot1q-tunnel

no switchport mode

Parameter description

Parameter	Description
no	Delete corresponding 802.1Q tunneling interface configuration.

Default configuration

No 802.1Q tunneling interface.

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface gi 0/1
DGS-3610(config-if)# switchport access vlan 22
DGS-3610(config-if)# switchport mode dot1q-tunnel
DGS-3610(config)# end
```

Related commands	**show vlan private-vlan**
Platform description	The software version must be later than v10.1.

12.1.2 switchport mode uplink

Set the port mode as uplink.

switchport mode uplink

no switchport mode

Parameter description

Parameter	Description
no	Cancel the setting of the uplink port mode.

Default configuration	No uplink port.
Command mode	Interface configuration mode

Examples

```
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# switchport mode up-link
DGS-3610(config)# end
```

Related commands	**show vlan private-vlan**
Platform description	The software version must be later than v10.1.

12.1.3 frame-tag tpid *tpid*

Set the manufacturer tpid.

frame-tag tpid <*tpid*>

no frame-tag tpid

Parameter description

Parameter	Description
no	Cancel the setting.

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface g0/3
DGS-3610(config-if)# frame-tag tpid 9100
DGS-3610(config-if)# end
DGS-3610# show frame-tag tpid
Port    tpid
------  ---------
Gi0/3   0x9100
```

Related commands

show frame-tag tpid

Platform description

The software version must be later than v10.1.

12.1.4 inner-priority-trust enable

Apply/cancel to copy the external tag priority of the interface message from internal tag.

inner-priority-trust enable

no inner-priority-trust enable

Parameter description

Parameter	Description
no	Cancel to copy the external tag priority of interface message from the internal tag.

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitEthernet 0/2
DGS-3610(config-if)# inner-priority-trust enable
```

Related commands

show inner-priority-trust

Platform description	The software version is v10.1 or later.

12.2 Showing Commands

- **show frame-tag tpid**
- **show inner-priority-trust**

12.2.1 show frame-tag tpid

Show the configuration of private VLAN.

show frame-tag tpid [**interface <***interface***>**]

Parameter description

Parameter	Description
<interface>	Specific Interface

Default configuration	The tpid is not modified.
Command mode	Privileged mode.

Examples

```
DGS-3610# show frame-tag tpid
DGS-3610# show frame-tag tpid interface gi0/1
Port    tpid
-----  ---------
Gi0/1  0x9100
```

Platform description	The software version must be later than v10.1.

12.2.2 show inner-priority-trust

Show the priority copy configuration.

show inner-priority-trust

Parameter description	None
Default	Non Copied

configuration	
Command mode	Privileged mode
Examples	DGS-3610# **show inner-priority-trust** Port inner-priority-trust **---- ----------** Gi0/1 enable
Platform description	The software version must be later than v10.1.

13 Configuring MAC Address Commands

13.1 Configuration Related Commands

The MAC address configuration commands include:

- **mac-address-table aging-time**
- **clear mac-address-table dynamic**
- **clear mac-address-table filtering**
- **clear mac-address-table static**
- **mac-address-table static**
- **mac-address-table filtering**
- **mac-address-table notification**
- **nmp trap mac-notification**
- **address-bind**
- **mac-manage-learning uniform**
- **mac-manage-learning uniform learning-synchronization**
- **mac-manage-learning dispersive**

13.1.1 mac-address-table aging-time

Specify the aging time of the MAC address. Use the **no** form of the command to restore the default setting.

mac-address-table aging-time *seconds*

no mac-address-table aging-time

Parameter description

Parameter	Description
seconds	The aging time, measured in seconds. The range is decided by 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-address-table.
Examples	`DGS-3610(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 the dynamic MAC address.

13.1.2 clear mac-address-table dynamic

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 all the specified dynamic MAC address.
interface *interface-id*	Clear all the dynamic MAC addresses on specified interface.
vlan *vlan-id*	Clear all the dynamic MAC addresses on specified VLAN.

Command mode	Privileged mode.
Usage guidelines	Use **show mac-address-table dynamic** to display all the dynamic MAC address tables.
Examples	Clear all the dynamic MAC address:

```
DGS-3610# clear mac-address-table dynamic
```

Related commands

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

13.1.3 clear mac-address-table filtering

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 on the specified VLAN.

Command mode

Privileged mode.

Usage guidelines

Use **show mac-address-table filtering** to display all the information in the filtering table.

Examples

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

```
DGS-3610# clear mac-address-table filtering address 00d0.f800.0c0c
```

Related commands

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

Platform description

13.1.4 clear mac-address-table static

Use this command to clear the setting static address table.

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

Parameter description

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

Command mode

Privileged mode.

Usage guidelines

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

Examples

The example below clears the static MAC address 00d0.f800.073c**:**

```
DGS-3610# clear mac-address-table static address
00d0.f800.073c
```

Related commands

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

13.1.5 mac-address-table static

Use this command to configure a static address. Use the **no** form of the command to remove a static 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	Specify the destination MAC address.
vlan-id	Specify the VLAN ID.

	interface-id	Specify the interface which the packets will be forwarded to.(it can be physical port or aggregate port)

Default configuration	No static address by default.
Command mode	Global configuration mode.
Usage guidelines	Static address has the same function as the dynamic address learnt by the device, but the static address will never be aged out, and it can only be configured and removed manually. Even if the switch is reset, the static address will not be lost. The static address should not be set as a multicast address. Use **show mac-address-table static** to display the configuration of static address table. Use **clear mac-address-table static** to clear the configuration of static MAC address.
Examples	When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified port gigabitethernet 1/1: `DGS-3610(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 address.
	clear mac-address-table static	Clear the static address.

13.1.6 mac-address-table filtering

Configure the filtering address. Use the **no** form of the command to remove the filtering address.

mac-address-table filtering *mac-address* **vlan** *vlan-id*

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

Parameter description

Parameter	Description
mac-address	Filtering Address
vlan *vlan-id*	VLAN ID, the range is defined by the device.

Default configuration

None.

Command mode

Global configuration mode.

Usage guidelines

The filtering address shall not be multicast address. Use **show mac-address-table filtering** to display the setting of filtering addresses.

Examples

```
DGS-3610(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 information of filtering address table.

13.1.7 mac-address-table notification

Enable MAC 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 for sending MAC address traps. Default value is 1 second.
history-size *value*	Specify the maximum number of the entries in MA-address-notification table. Default value is 50.

Default

The default interval is 1 second; the maximum number of the entries

configuration	in the table is 50.
Command mode	Global configuration mode.
Usage guidelines	MAC address notifications are generated only for dynamic address and security address, and traps are not generated for static addresses. In global configuration mode, you can use the **snmp-server enable traps mac-notification** to enable or disable the trap function for sending MAC address of the device..

Examples

```
DGS-3610(config)# mac-address-table notification
DGS-3610(config)# mac-address-table notification interval 40
DGS-3610(config)# mac-address-table notification history-size 100
```

Related commands

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

13.1.8 snmp trap mac-notification

Enable the MAC address 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 adding an address
removed	Notify when removing an address

Default configuration	Disabled this function by default.
Command mode	Interface configuration mode.

Usage guidelines

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

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(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 notification configuration and the notification table.

13.1.9 address-bind

Use this command to configure a binding between an IP address and a MAC address. .

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 to a specified MAC address, when the device receives the frame with the same IP address, and when the source MAC address of the frame is not the MAC bound for the IP address, it will discard by the device.

Examples

The following example binds the IP address 3.3.3.3 to the MAC address 00d0.f811.1112.

```
DGS-3610(config)# address-bind 3.3.3.3 00d0.f811.1112
```

Related commands

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

13.1.10 address-bind *ip-address*

Use this command to configure a binding between an IP address and a MAC address.

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 to a specified MAC address, when the device receives the frame with the same IP address, and when the source MAC address of the frame is not the MAC bound for the IP address, it will discard by the device.

Examples

The following example binds the IP address 3.3.3.3 to the MAC address 00d0.f811.1112.

```
DGS-3610(config)# address-bind 3.3.3.3 00d0.f811.1112
```

Related commands

Command	Function
show address-bind	Show the binding table.

13.1.11 address-bind uplink

Use this command to configure a binding between an IP address and a MAC address.

address-bind uplink *intf-id*

no address-bind uplink *intf-id*

Parameter description

Parameter	Description
intf-id	An interface to be set as an exceptional port

Command mode	Global configuration mode.
Usage guidelines	If you have bound an IP address to a specified MAC address, when the switch receives packets with the same IP address and a different source MAC address bound for the IP address, it will discard these packets. 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 to the binding of an address DGS-3610(config)#**address-bind uplink** *fa0/1*

Related commands

Command	Function
show address-bind uplink	Exceptional port of the binding address

Platform description	Version later than v10.1

13.1.12 address-bind install

Install/uninstall the exceptional port policy:

address-bind install

no address-bind install

Parameter description	None
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	Bind the address to the fa 0/1 port: `DGS-3610(config)# address-bind uplink fa0/1`

	`DGS-3610(config)# address-bind install`

Related commands	**Command**	**Function**
	show address-bind uplink	Show the exceptional port of the binding address

Platform description	Version later than v10.1

13.1.13 mac-manage-learning uniform

This command sets the management and learning mode of the dynamic MAC address to the uniform mode.

Parameter description	None
Command mode	Global configuration mode.
Usage guidelines	Setting the management and learning mode of the dynamic MAC address to the uniform mode can raise the L2 switching efficiency. After changing the MAC learning mode, you must save it and restart before the new mode takes effect.
Examples	None

Related commands	**Command**	**Function**
	show mac-address-table mac-manage-learning	Show the MAC management and learning mode

13.1.14 mac-manage-learning uniform learning-synchronization

This command synchronizes the dynamic MAC address in the whole device in the uniform mode.

no mac-manage-learning uniform learning-sychronization

Parameter description	None
Command mode	Global configuration mode.
Usage guidelines	In the uniform mode, the synchronization of the dynamic MAC address in the whole device can further raise the L2 switching efficiency. You can use the **no** form of this command to cancel the synchronization.
Examples	None

Related commands

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

13.1.15 mac-manage-learning dispersive

This command sets the management and learning mode of the dynamic MAC address to the dispersive mode.

Parameter description	None
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	None.

	Command	Function
Related commands	**show mac-address-table mac-manage-learning**	Show the MAC address management and learning mode

13.2 Showing Related Command

The MAC address showing commands include:

- **show mac-address-table address**
- **show mac-address-table aging-time**
- **show mac-address-table count**
- **show mac-address-table dynamic**
- **show mac-address-table filtering**
- **show mac-address-table interface**
- **show mac-address-table notification**
- **show mac-address-table static**
- **show mac-address-table vlan**
- **show address-bind**
- **show mac-address-table mac-manage-learning**

13.2.1 show mac-address-table address

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

```
DGS-3610# 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 for the specified interface
show mac-address-table vlan	Show all types of MAC addresses for the specified VLAN
show mac-address-table count	Show the address count 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.

13.2.2 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

```
DGS-3610# show mac-address-table aging-time
Aging time   : 300
```

Related commands

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

13.2.3 show mac-address-table count

Show the address count in the MAC address table.

show mac-address-table count

Command mode	Privileged mode.

Examples

```
DGS-3610# 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	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 the specified all types of MAC address.
show mac-address-table interface	Show all types of MAC addresses for the specified interface
show mac-address-table vlan	Show all types of MAC addresses for the specified VLAN

13.2.4 show mac-address-table dynamic

Display dynamic address table information.

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

Parameter description

Parameter	Description
mac-addr	Specify the destination MAC address.
vlan-id	Specify the VLAN corresponding to the table.
interface-id	The interface the packet is forwarded to. (It may be the physical port or AggregatePort)

Default configuration	Show all the information.

Command mode	Privileged mode.

Examples

```
DGS-3610# 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 address.

13.2.5 show mac-address-table filtering

Show the filtering address table.

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

Parameter description

Parameter	Description
mac-addr	Specify the destination MAC address.
lan-id	Specify the VLAN ID.

Command mode	Privileged mode.

Examples

```
DGS-3610# 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 MAC address.

13.2.6 show mac-address-table interface

Show all the address information on a specified interface (including static address and dynamic addresses).

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

Parameter description

Parameter	Description
interface-id	The specified interface(physical interface or aggregate port).
vlan-id	Specify the VLAN ID.

Command mode

Privileged mode.

Examples

```
DGS-3610# 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 the specified all types of MAC address.
show mac-address-table vlan	Show all types of MAC addresses for the specified VLAN
show mac-address-table count	Show the address counts in the MAC address table.

13.2.7 show mac-address-table notification

Show the MAC notification configuration and the notification table.

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

Parameter description

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

Default configuration

By default, all the MAC address notification settings are shown.

Command mode

Privileged mode.

Examples

```
DGS-3610# show mac-address-table notification interface
Interface        MAC Added Trap  MAC Removed Trap
---------         --------------      --------------
GigabitEthernet1/14   Disabled       Disabled
DGS-3610# 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
DGS-3610# 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 function.
snmp trap mac-notification	Enable the MAC address notification trap on the specified interface.

13.2.8 show mac-address-table static

Show the static address.

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

Parameter description

Parameter	Description
mac-addr	Specify the destination MAC address the entry corresponding to.
vlan-id	Specify the VLAN corresponding to entry..
interface-id	Forwording the packet to the interface

	(physical interface or aggregate port)

Command mode

Privileged mode.

Examples

Show only static addresses

```
DGS-3610# 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 address.
clear mac-address-table static	Clear the static address.

13.2.9 show mac-address-table vlan

Show all types of MAC addresses for the specified VLAN

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

Parameter description

Parameter	Description
vlan-id	Specified VLAN ID.

Command mode

Privileged mode.

Examples

```
DGS-3610# 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 the specified all types of MAC address.
	show mac-address-table interface	Show all types of MAC addresses for the specified interface
	show mac-address-table count	Show the address counts in the MAC address table.

13.2.10 show address-bind

Use this command to display the address binding.

show address-bind

Command mode	Privileged mode.
Usage guidelines	None.

Examples

```
DGS-3610# 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	Specify the address to be bound.

13.2.11 show mac-address-table mac-manage-learning

This command shows the management and learning mode of the dynamic MAC address.

Command mode	Privileged mode.
Usage guidelines	None.

Examples

```
DGS-3610# 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-learing 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

14 Configuring DHCP Snooping Command

14.1 DHCP snooping Global Commands

The following commands are available in the DHCP snooping global mode:

- **ip dhcp snooping**
- **ip dhcp snooping veritfy mac-address**
- **ip dhcp snooping binding**
- **ip dhcp snooping database wirte-delay**
- **ip dhcp snooping database wirte-to-flash**
- **ip dhcp snooping information option**
- **ip dhcp snooping address-bind**

14.1.1 ip dhcp snooping

To use the DHCP snooping function, 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	None.
Default	The DHCP snooping global switch is disabled.
Command mode	Global configuration mode.
Usage guidelines	Set the switch to enable the DHCP snooping function, you can use the **show ip dhcp snooping** command view whether the DHCP snooping function is enabled.

Examples

The following example shows how to enable the DHCP snooping.

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping
DGS-3610(config)# end
DGS-3610# show ip dhcp snooping

Switch DHCP snooping status: enable
Verification of hwaddr field status: disable
DHCP snooping database write-delay time: 0(not wirte)
Interface                Trusted
-----------------------  -------
FastEthernet0/11         yes
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of DHCP snooping.

14.1.2 ip dhcp snooping verify mac-address

Set the switch to check whether the source MAC address of the DHCP request message matches with the client addr field in the DHCP message, and he **no** form of this command can be used to disable the check of the source MAC for the message.

[**no**] **ip dhcp snooping verify mac-address**

Parameter description

None.

Default

The check of the message source MAC is disabled.

Command mode

Global configuration mode.

Usage guidelines

Configure this command to enable to check the validity of the source MAC for the DHCP message. Once the source mac check is enabled, the DHCP request message which fails to pass the source mac check will be discarded.

Examples

The following example shows how to enable the source MAC check of the DHCP message.

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping verify mac-address
DGS-3610(config)# end
```

```
DGS-3610# show ip dhcp snooping

Switch DHCP snooping status: enable
Verification of hwaddr field status: enable
DHCP snooping database write-delay time: 0(not wirte)
Interface                Trusted
-----------------------  -------
FastEthernet0/11         yes
```

Related commands	Command	Description
	show ip dhcp snooping	View the configuration information of the DHCP snooping.

14.1.3 ip dhcp snooping binding

Add the static user information of the DHCP snooping, and the **no** form of this command can be used to delete corresponding static users.

[**no**] **ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* **ip**

ip-address **interface** *interface-id*

Parameter description

Parameter	Description
mac-address	The MAC address of users who are added statically
vlan-id	The vlan id of users who are added statically
ip-address	The IP address of users who are added statically
interface-id	The port from which the users are added statically

Default

No address of static users is added.

Command mode

Global configuration mode.

Usage guidelines

Add the static DHCP user information to the DHCP snooping binding database by configuring this command.

Examples

The following example shows how configure a static user to port 1.

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping binding 00d0.f801.0101 vlan 1 ip
192.168.4.243 interface fastEthernet 0/1
```

```
DGS-3610(config)# end
DGS-3610# show ip dhcp snooping binding
Total number of bindings: 1
 acAddress     IpAddress     Lease(sec)   Type  VLAN  Interface
----------     ----------    ----------   ---------  ----------
00d0f8010101   192.168.4.1   -            STATIC  1   Fa 0/1
```

Related commands	Command	Description
	show ip dhcp snooping binding	View the information of the DHCP snooping binding database.

14.1.4 ip dhcp snooping information option

This command enables the DHCP snooping information option function. The **no** form of this command disables this function.

[no] ip dhcp snooping information option

Default configuration	None.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The function of DHCP snooping information option can be enabled by configuring this command

Examples	Set a static user to port 1:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# ip dhcp snooping information option`
	`DGS-3610(config)# end`

Related commands	Command	Function
	ip dhcp relay information option82	To configure the enabling function of dhcp relay information option

14.1.5 ip dhcp snooping database write-delay

Configure the switch to write the user information of the DHCP snooping binding database into the flash timely, and the **no** form of this command will set the time as 0, namely, the information will be written into the flash at random.

[**no**] **ip dhcp snooping database write-delay** *time*

Parameter description

Parameter	Description
time	The time interval between the operations to write the DHCP snooping database information into the flash for two times.

Default

0, indicated to write the user information to flash at random.

Command mode

Global configuration mode.

Usage guidelines

Set the time interval to write the information to flash on the switch, which can be viewed by the **show ip dhcp snooping** command.

Examples

The following example shows how to set the time interval at which the switch writes information to the flash as 3600:

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping database
write-delay 3600
DGS-3610(config)# end
DGS-3610# show ip dhcp snooping
Switch DHCP snooping status: enable
Verification of hwaddr field status: enable
DHCP snooping database write-delay time: 3600
Interface                Trusted
-----------------------  -------
FastEthernet0/11         yes
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

14.1.6 ip dhcp snooping database write-to-flash

Write the dynamic user information of the DHCP binding data for the switch into flash.

ip dhcp snooping database write-to-flash

Parameter description	This command has no parameters.
Default	No default.
Command mode	Global configuration mode.
Usage guidelines	Use this command to write the dynamic user information of the DHCP binding data for the switch into flash.

Examples	The following example shows how to write the dynamic user information of the DHCP binding data for the switch into flash.
	`DGS-3610# configure terminal`
	`DGS-3610(config)# ip dhcp snooping database write-to-flash`
	`DGS-3610(config)# end`
	`DGS-3610#`

Related commands	None.

14.2 DHCP snooping Interface Mode Commands

There are several commands under the DHCP snooping interface mode as follows:

- **ip dhcp snooping trust**
- **ip dhcp snooping address-bind**

14.2.1 ip dhcp snooping trust

Use this command to set the port of the switch as the TRUST port.

[**no**] **ip dhcp snooping trust**

Parameter description	None.
Default	All of the ports are the UNTRUST ports.

Command mode	Interface configuration mode.
Usage guidelines	Use this command set the port as the DHCP snooping TRUST port in corresponding interface mode.

Examples	The following example shows how to set port 1 as the trust port:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface fastEthernet 0/1`
	`DGS-3610(config-if)# ip dhcp snooping trust`
	`DGS-3610(config-if)# end`
	`DGS-3610# show ip dhcp snooping`
	`Switch DHCP snooping status: enable`
	`Verification of hwaddr field status: enable`
	`DHCP snooping database write-delay time: 3600`
	`Interface Trusted`
	`----------- -------`
	`FastEthernet0/1 yes`

Related commands	**Command**	**Description**
	show ip dhcp snooping	View the configuration information of the DHCP snooping.

14.2.2 ip dhcp snooping address-bind

Enable the address binding function of DHCP snooping, the **no** form of this command can disable the corresponding configuration.

[no] ip dhcp snooping address-bind

Parameter description	None.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	Enable the address binding function of DHCP snooping by configuring this command.

Examples	Set a static user to port 1:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface fastEthernet 0/1`
	`DGS-3610(config-if)# ip dhcp snooping address-bind`
	`DGS-3610(config-if)# end`

Related commands	**Command**	**Function**
	switchport port-security arp-check	Enable **arp check** function of the port.

14.3 Other configuration commands of DHCP snooping

The configuration of other dhcp snooping includes the commands as follows:

- **clear ip dhcp snooping binding**

14.3.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information in the DHCP snooping binding database.

clear ip dhcp snooping binding

Parameter description	None.
Default	None.
Command mode	Privileged mode.
Usage guidelines	If users want to clear current DHCP snooping dynamic user information, use this command.

Examples	The following example demonstrates how to clear the dynamic database information in the DHCP snooping.
	`DGS-3610# clear ip dhcp snooping binding`
	`DGS-3610# show ip dhcp snooping binding`
	`Total number of bindings: 0`
	`MacAddress IpAddress Lease(sec) Type VLAN Interface`
	`---------- ---------- ---------- -------- ---- ----------`

	Command	Description
Related commands	**show ip dhcp snooping binding**	Show the database information in the DHCP snooping binding.

14.4 DHCP snooping Show Commands

- **show ip dhcp snooping**
- **show ip dhcp snooping binding**

14.4.1 show ip dhcp snooping

View the setting of the dhcp snooping.

show ip dhcp snooping

Parameter description	This command has no parameters.
Default	None
Command mode	Privileged mode.
Usage guidelines	None.

Examples	The following is a show example.
	`DGS-3610# show ip dhcp snooping`
	
	`Switch DHCP snooping status: enable`
	`Verification of hwaddr field status: enable`
	`DHCP snooping database write-delay time: 3600`
	`InterfaceTrusted`
	`-------------------------`
	`FastEthernet0/11yes`

	Command	Description
Related commands	**ip dhcp snooping**	DHCP snooping global configuration switch
	ip dhcp snooping binding mac-address	Source mac check switch of DHCP snooping message

	ip dhcp snoooping write-delay	Configure the interval of the delay to write into flash.
	ip dhcp snooping binding	Set the port as a DHCP snooping trust port.

14.4.2 show ip dhcp snooping binding

This command is used to view the information of the dhcp snooping binding database.

show ip dhcp snooping binding

Parameter description	None.
Default	None.
Command mode	Privileged mode.
Usage guidelines	None.

Examples	The following is a show example:
	`DGS-3610# show ip dhcp snooping binding`
	`Total number of bindings: 0`
	`MacAddressIpAddressLease(sec)TypeVLANInterface`
	`----------`

Related commands	**Command**	**Description**
	ip dhcp snooping binding	Set the DHCP snooping static users.
	clear ip dhcp snooping binding	Clear the dynamic user information in the DHCP snooping.

15 Configuring IGMP Snooping Commands

15.1 Configuring Related Commands

IGMP Snooping includes profile mode and global mode configuration commands.

Profile mode commands include:

- **deny**
- **permit**
- **range**

Configuration mode commands include:

- **ip igmp profile**
- **ip igmp snooping filter**
- **ip igmp snooping ivgl**
- **ip igmp snooping ivgl-svgl**
- **ip igmp snooping limit-ipmc vlan**
- **ip igmp snooping max-groups**
- **ip igmp source-check default-server**
- **ip igmp source-check port**
- **ip igmp snooping svgl**
- ip igmp snooping fast-leave enable
- ip igmp snooping fast-leave enable
- **ip igmp snooping vlan mrouter interface**
- **ip igmp snooping vlan mrouter interface profile**
- **ip igmp snooping vlan mrouter learn**
- **ip igmp snooping vlan static**

15.1.1 deny

To prohibit from forwarding the multicast flow in the range specified by profile, execute the **deny** configuration command in the profile mode.

deny

Parameter description

No parameters

Level Keyword	Description
deny	Prohibit from forwarding the multicast address in the range specified by profile

Default

The profile performs the deny operation by default.

Command mode

profile configuration mode.

Usage guidelines

First, configure the multicast range using the **range** command in the profile mode. In addition, the profile must be applied to the interface in order to make the profile configuration to take effective.

Examples

The following example shows how to prohibit from forwarding the profile of 224.2.2.2 multicast stream:

```
DGS-3610(config)# ip igmp profile 1
DGS-3610(config-profile)# range 224.2.2.2
DGS-3610(config-profile)# deny
```

Related commands

Command	Description
ip igmp profile	Creates a profile
range	Configures multicast address range

15.1.2 permit

To limit the range of profile multicast stream, execute the **permit** configuration command in the profile mode. This way the interface associated with this profile will forward the specified multicast stream only.

permit

Parameter description

No parameters

Level Keyword	Description
permit	Allow to forward the multicast address in the range specified by profile

Default

The profile perform the deny operation by default.

Command mode

Profile configuration mode.

Usage guidelines

First, configure the multicast range using the **range** command in the profile mode. In addition, the profile must be applied to the interface in order to make the profile configuration to take effective.

Examples

The following example shows how to allow to forward the profile of 224.2.2.2 multicast stream:

```
DGS-3610(config)# ip igmp profile 1
DGS-3610(config-profile)# range 224.2.2.2
DGS-3610(config-profile)# permit
```

Related commands

Command	Description
ip igmp profile	Create a profile
range	Configure multicast address range

15.1.3 range

To specify the range of profile multicast stream, execute the **range** command in the profile 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 IP address.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter description

Parameter	Description
low-ip-address	Specify the start address of a range.
high-ip-address	Specify the end address of a range.

Default

No default.

Command mode

profile configuration mode.

Usage guidelines

You can specify an operation after configuring the address range. The operation of profile is denied by default. In addition, the profile must be applied to the interface in order to make the profile configuration to take effective.

Examples

The following example shows how to create multicast stream profile in the range 224.2.2.2~224.2.2.244:

```
DGS-3610(config)# ip igmp profile 1
DGS-3610(config-profile)# range 224.2.2.2 224.2.2.244
```

Related commands

Command	Description
ip igmp profile	Create a profile
deny	Specify the operation of profile as deny
permit	Specify the operation of profile as permit

15.1.4 ip igmp profile

This is a mode navigation command. Use this command to select *profile-number* 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, ranging 1-65535

Default

No default

Command mode

Global configuration mode.

Usage guidelines

The profile must be applied to the specified interface in order to make the profile to take effective.

Examples

The following example shows how to create a profile numbered 1 and enter the profile configuration mode.

```
DGS-3610(config)# ip igmp profile 1
DGS-3610(config-profile)#
```

Related commands

Command	Description
range	Configure multicast address range

15.1.5 ip igmp snooping filter

To configure a port to receive a specific set of multicast data streams, execute this command in the interface mode to associate 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 No default.

Command mode Interface configuration mode.

Usage guidelines A specific profile must be created before the filter can be associated.

Examples The following example demonstrates how to associate profile 1 on a megabit port 0/1:

```
DGS-3610(config)# interface fastEthernet 0/1
DGS-3610(config-if)# ip igmp snooping filter 1
```

Related commands

Command	Description
ip igmp profile	Creating a profile

15.1.6 ip igmp snooping ivgl

To enable igmp snooping and specify the ivgl mode, execute the global configuration command **ip igmp snooping ivgl**. The **no** form of this command is used to disable igmp snooping.

ip igmp snooping ivgl

no ip igmp snooping

Parameter description No parameters.

Default disable mode.

Command mode	Global configuration mode.
Usage guidelines	After this mode is set, for multicast frames in different VLANs but with the same multicast address, **igmp snooping** only handles the same group in the multicast address table (GDA), while other multicast frames will be forwarded.
Examples	The following example demonstrates how to enable igmp snooping and set the ivgl mode: `DGS-3610(config)# ip igmp snooping ivgl`

Related commands

Command	Description
ip igmp snooping svgl	Enable **igmp snooping** and configure the svgl mode
ip igmp snooping ivgl-svgl	Enable **igmp snooping** and configure the hybrid mode

15.1.7 ip igmp snooping ivgl-svgl

To enable igmp snooping and specify the ivgl-svgl mode, execute the global configuration command **ip igmp snooping ivgl-svgl**. The **no** form of this command is used to disable igmp snooping.

ip igmp snooping ivgl-svgl

no ip igmp snooping

Parameter description	No parameters.
Default	Disable mode.
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 set the ivgl-svgl mode on the device:

```
DGS-3610(config)# ip igmp snooping ivgl-svgl
```

Related commands

Command	Description
ip igmp snooping svgl	Enable **igmp snooping** and configure the svgl mode
ip igmp snooping ivgl	Enable **igmp snooping** and configure the ivgl mode

15.1.8 ip igmp snooping limit-ipmc vlan server

To add a multicast source IP checklist entry, execute the global configuration command **ip igmp snooping limit-ipmc vlan**. 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 checklist entry.
Gaddress	Multicast address.
Saddress	Multicast source address (multicast server).

Default

No default

Command mode

Global configuration mode.

Usage guidelines

The source IP check function must be enabled before an entry can be added.

Examples

The following example shows how to add a multicast source IP filter table entry.

```
DGS-3610(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	Configure a default source IP while enabling the IP check.

	default-server	

15.1.9 ip igmp snooping max-groups

To configure the maximum number of groups that can be added dynamically to this interface, execute the interface configuration command **ip igmp snooping max-groups**. The **no** form of this command is used to cancel the maximum groups limit.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

Parameter description	**Parameter**	**Description**
	number	The parameter ranges between 0 and 4294967294.

Default	No limit.
Command mode	Interface configuration mode.
Usage guidelines	If a maximum number of groups are configured, the device will no longer receive and process IGMP Report packets when the number of groups on this interface is beyond the range.

Examples	The following example shows how to configure the megabit interface 0/1 to process 100 multicast groups only:
	`DGS-3610(config)# interface fastEthernet 0/1`
	`DGS-3610(config-if)# ip igmp snooping max-group 100`

Related commands	**Command**	**Description**
	ip igmp snooping filter	Filter multicast groups that pass through a port

15.1.10 ip igmp source-check default-server

Source-IP-check is used to require that one or several IPMC flows should only be supplied by the server with an IP address.

To configure the source IP check function of igmp snooping, execute the global configuration command **ip igmp source-check default-server**. The **no** form of this command is used to disable the source IP check function.

ip igmp source-check default-server *address*

no ip igmp souce-check

Parameter description

Parameter	Description
address	Default multicast source address (default multicast server address).

Default This function is disabled by default.

Command mode Global configuration mode.

Usage guidelines The IP check is a global switch. Once it is enabled, all the IPMC streams must conform to the specified address. Otherwise, they will be discarded. The device allow users to configure the source IP of all IPMC flows that we call it default multicast server. The default server address must set along with enabling the source-IP-check.

Examples The following example shows how to enable the multicast source IP check function and configure a default source IP address.

```
DGS-3610(config)# ip igmp 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 checklist.

15.1.11 ip igmp source-check port

The source port check function is used to specify a certain or several IPMC streams to be provided by the mroute interface only. To configure the source port check function of igmp snooping, execute the global configuration command **ip igmp source-check port**. The **no** form of this command is used to disable the source port check function.

ip igmp source-check port

no ip igmp source-check port

Parameter description No parameters

Default	This function is disabled by default.
Command mode	Interface configuration mode..
Usage guidelines	The source port check function is a global switch. Once it is turned on, all the IPMC streams must come from the mroute interface. Otherwise, they will be discarded.
Examples	The following example shows how to enable the source port check function of igmp snooping. `DGS-3610(config)# ip igmp snooping source-check port`

Related commands

Command	Description
Ip igmp snooping source-check default-server	Enable the multicast source IP check function.

15.1.12 ip igmp snooping svgl

To enable igmp snooping and specify the svgl mode, execute the global configuration command **ip igmp snooping svgl**. The **no** form of this command is used to disable igmp snooping.

ip igmp snooping svgl

no ip igmp snooping

Parameter description	No parameters
Default	disable mode.
Command mode	Global configuration mode.
Usage guidelines	The multicast address range of the SVGL mode must be configured before the SVGL mode can work normally.
Examples	The following example demonstrates how to enable igmp snooping

and set the svgl mode:

```
DGS-3610(config)# ip igmp snooping svgl
```

Related commands

Command	Description
ip igmp snooping ivgl	Enable **igmp snooping** and configure the ivgl mode
ip igmp snooping ivgl-svgl	Enable **igmp snooping** and configure the hybrid mode

15.1.13 ip igmp snooping vlan mrouter interface

Router interface is a port through which a multicast device is connected to a device. To configure a multicast router interface, execute the global configuration command **ip igmp snooping vlan mrouter interface**. The **no** form of this command is used to delete a router 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	Configure the VLAN ID of a router interface.
interface-id	Interface id.

Default

No default.

Command mode

Global configuration mode.

Usage guidelines

When the source port check is on, only the multicast flows entering through the router interface are forwarded, and other flows will be discarded.

Examples

The following example demonstrates how to configure a multicast router interface on the equipment:

```
DGS-3610(config)# ip igmp snooping vlan 1 mrouter interface fastEthernet 0/1
```

Related commands

Command	Description
ip igmp snooping	Multicast source port check

	source-check port	

15.1.14 ip igmp snooping vlan mrouter interface profile

By default, the router interface forwards the multicast data flow as the member of all multicast addresses within this VLAN. But it is possible that some multicast data is not expected to be forwarded to the multicast device. The administrator can use the IGMP Profile to filter the range of multicast data to be forwarded by the router interface. To limit the multicast forward range, execute the global configuration command **ip igmp snooping vlan mrouter interface profile**. The **no** form of this command is used to eliminate the association between a port and a profile.

ip igmp snooping vlan *vid* **mrouter interface** *interface-id* **profile** *profile-num*

no ip igmp snooping vlan *vid* **mrouter interface** *interface-id* **profile**

Parameter description

Parameter	Description
vid	VLAN ID of a router interface.
interface-id	Interface ID.
profile-num	Specified profile number

Default

No default.

Command mode

Global configuration mode.

Usage guidelines

A profile must be created first. After association, only the multicast flows complying with this profile can be forwarded to this router interface.

Examples

The following example demonstrates how to associate a profile to a multicast router interface:

```
DGS-3610(config)# ip igmp snooping vlan 1 mrouter interface fastEthernet 0/1 profile 1
```

Related commands

Command	Description
ip igmp snooping vlan mrouter interface	Configure a multicast router interface

15.1.15 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 router interface, execute the global configuration command **ip igmp snooping vlan mrouter learn**. 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 router interface.

Default

This function is disabled by default.

Command mode

Global configuration mode.

Usage guidelines

With the source port check function enabled, dynamic router interface learning will help improve the application flexibility of igmp snooping.

Examples

The following example demonstrates how to enable the dynamic router interface learning function on the equipment:

```
DGS-3610(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

Related commands

Command	Description
ip igmp snooping vlan mrouter interface	Configure a multicast router interface

15.1.16 ip igmp snooping dyn-mr-aging-time

To configure the aging time of the router interface in dynamic learning.

ip igmp snooping dyn-mr-aging-time *time*

no ip igmp snooping dyn-mr-aging-time

Parameter description

Parameter	Description
time	The aging time of the router interface in dynamic learning

Default configuration	300s.
Command mode	Global configuration mode.
Usage guidelines	When the learning of the dynamic router interface is enabled, this command sets the aging time of the dynamic router interface. If the aging time is set too short, the routes may be added and deleted frequently.
Examples	Set the aging time for the dynamic learning of the router interface to 100 s: `DGS-3610(config)# ip igmp snooping dyn-mr-aging-time 100`

Related commands

Command	Function
ip igmp snooping	Configure a multicast router interface

15.1.17 ip igmp snooping vlan static interface

With igmp snooping enabled, when a port is configured statically to receive a certain multicast stream, it will not be affected various IGMP packets. Execute the global configuration command **ip igmp snooping vlan static interface**. 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 router interface.
ip-addr	multicast address
interface-id	Interface ID.

Default	No default
Command mode	Global configuration mode.

Usage guidelines	Multiple multicast addresses can be configured for an interface.
Examples	The following example demonstrates how to configure a static multicast address on a port: `DGS-3610(config)# ip igmp snooping vlan 1 static 224.0.0.2 interface fastEthernet 0/1`

Related commands	**Command**	**Description**
	ip igmp snooping vlan mrouter interface	Configure a multicast router interface

15.1.18 ip igmp snooping fast-leave enable

To enable **igmp snooping fast-leave**, run the global configuration command **ip igmp snooping fast-leave enable**. The **no** form of this command is used to disable igmp snooping.

ip igmp snooping fast-leave enable

no ip igmp snooping fast-leave enable

Parameter description	No parameters.
Default configuration	Disable mode.
Command mode	Global configuration mode.
Usage guidelines	After this command is run, the fast-leave function is enabled and the corresponding group is deleted from the corresponding port when the IGMP leave packets are received.
Examples	The following example demonstrates how to enable `igmp snooping fast-leave` on the device: `DGS-3610(config)# ip igmp snooping fast-leave`
Related	None.

commands	

15.1.19 ip igmp snooping suppression enable

To enable igmp snooping suppression, please execute the global configuration command **ip igmp snooping suppression enable**. 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	No parameters
Default configuration	Disable mode.
Command mode	Global configuration mode.
Usage guidelines	After this command is run, the suppression function is enabled, and the switch begins to suppress the **IGMP v1/v2** report packets.
Examples	The following example demonstrate how to enable igmp snooping suppression on the device: `DGS-3610(config)# ip igmp snooping suppression`
Related commands	None.

15.1.20 ip igmp snooping query-max-resposne-time

You can set the time for the switch to wait the members to join the group messages after the switch received the **query** message. If the message for the members to join the group is not received after the set time, the members are deemed left and then are deleted.

ip igmp snooping query-max-resposne-time *time*

no ip igmp snooping query-max-resposne-time

Parameter	**Parameter**	**Description**

description	*time*	The aging time of the router interface in dynamic learning.

Default configuration	10s.
Command mode	Global configuration mode.
Usage guidelines	You can set the time for the switch to wait the members to join the group messages after the switch received the query message. If the message for the members to join the group is not received after the set time, the members are deemed left and then are deleted. You can use this command to adjust the waiting time after the query message is received.
Examples	Set the aging time for the dynamic learning of the router interface to 100 s: `DGS-3610(config)# ip igmp snooping query-max-resposne-time 100`

Related commands	**Command**	**Function**
	ip igmp snooping	Configure a multicast router interface

15.1.21 Display and Monitoring Commands

It includes the following commands:

show igmp snooping [gda-table | interface | mrouter]

show igmp profile [*profile-number*]

debug igmp snooping

15.1.22 show igmp snooping

It shows information about igmp snooping.

show igmp snooping [gda-table | interface | mrouter| statistics [vlan *vlan-id*]]

Parameter	**Parameter**	**Description**

description	None	Show the function configuration of igmp snooping.
	gda-table	Show the multicast forwarding rule table.
	interface	Show the configuration of igmp snooping filtring.
	mrouter	Show the multicast router interface information
	statistics [**vlan** *vlan-id*]	Show the snooping statistics information

Command mode	Privileged mode.

15.1.23 show igmp profile [*profile-number*]

Parameter description	**Parameter**	**Description**
	none	Show the configuration information of profile.
	profile-number	show the specified configuration information of profile.

Command mode	Privileged EXEC configuration mode.

15.1.24 debug igmp snooping

It is used to turn on the igmp snooping service debugging switch. The **no** form of this command is used to turn off the debugging switch.

- **debug igmp snooping**
- **undebug igmp snooping**

Parameter description	No parameter or keyword.

Command mode	Privileged mode.

16 Configuration PSNP Command

16.1 Configuration Related Command

PSNP configuration includes following commands:

- **ip pim snooping** (global configuration mode)
- **ip pim snooping** (interface configuration mode)
- **show ip pim snooping**

16.1.1 ip pim snooping (global configuration mode)

This command is used to enable or disable the PIM snooping globally.

ip pim snooping

no ip pim snooping

Parameter description	None.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	If the PIM snooping function is disabled globally, the PIM snooping function of all VLANs will be invalid.
Examples	The following example disables the PIM snooping function: `DGS-3610(config)# no ip pim snooping`

Platform description	This command is enabled on the switch.

16.1.2 ip pim snooping (interface configuration mode)

This command is used to enable/disable the PIM snooping on the interface.

ip pim snooping

no ip pim snooping

Parameter description	None.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	To enable the PIM snooping on the interface, it is necessary to enable the PIM snooping globally. After the PIM snooping is disabled globally, the PIM snooping function of all interfaces will be invalid.

Examples	The following example demonstrates the function of PIM snooping:
	`DGS-3610(config)# interface vlan 100`
	`DGS-3610(config-if)# ip pim snooping`
	`DGS-3610(config-if)# end`

Platform description	This command is enabled on the switch.

16.1.3 show ip pim snooping

This command can display related information of PIM snooping.

show ip pim snooping

Parameter description	None.

Default configuration	None
Command mode	Privileged mode.
Usage guidelines	None.

Examples	The following example shows the related information of PIM snooping function:
	`DGS-3610# show` **`ip pim snooping`**
	`PIM Snooping table: 0 neighbour, Memory:8`
	`Interface VLAN 2(4098), PC:0`

Platform description	This command is enabled on the switch.

17 Configuring MSTP Commands

17.1 Configuring Related Commands

17.1.1 spanning-tree

Use this command to enable MSTP, and the parameters of the command can be used to enable MSTP and configure the MSTP global configuration simultaneously. Using the **no** form of the command will disable spanning-tree. The **no** form of the command with parameter option only returns the corresponding parameter to the default value, and will not disable spanning-tree.

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*	The time interval for the change of the port status.
hello-time *seconds*	The time interval when the equipment to send the BPDU message timely.
max-age *seconds*	The longest time for the BPDU message.

Default configuration

The **spanning-tree** is disabled, by default.

Command mode

Global configuration mode

Usage guidelines

The range among **forward-time, hello time and max-age** is interrelated. The modification of one of the three values shall affect the range of other two values. There is a restricted relationship among the above three value.
2*(Hello Time+1.0snd) <= Max-Age Time <=
2*(Forward-Delay–1.0snd)
The value that does not meet the condition can not be configured successfully.

Examples

Enable **spanning-tree**:

```
DGS-3610(config)# spanning-tree
Configure the BridgeForwardDelay
DGS-3610(config)# spanning-tree  forward-time 10
```

Related commands

Command	Description
show spanning-tree	Show the STP global configuration.
spanning-tree mst cost	Set the PathCost of an STP interface.
spanning-tree tx-hold-count	Set the global TxHoldCount of STP.

17.1.2 spanning-tree bpdufilter

Enable the BPDU filter feature of some interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU filter function of the interface.

spanning-tree bpdufilter [**enabled** | **disabled**]

Parameter description

Parameter	Description
enabled	Enable BPDU filter of the interface.
Disabled	Disable BPDU filter of the interface.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# spanning-tree bpdufilter enable
```

Related

Command	Description

commands	**show spanning-tree interface**	Show the STP port configuration.

17.1.3 spanning-tree bpduguard

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 of the interface.

spanning-tree bpduguard [**enabled** | **disabled**]

Parameter description

Parameter	Description
enabled	Enable BPDU guard of the interface.
disabled	Disable BPDU guard of the interface.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# spanning-tree bpduguard enable
```

Related commands

Command	Description
show spanning-tree interface	Show the STP port configuration.

17.1.4 spanning-tree link-type

Configure the link type of a interface to be point-to-point or not. Use the **no** form of the command to return 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	Set the link type of an interface to shared forcibly.

Default configuration	A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.
Command mode	Interface configuration mode.
Examples	`DGS-3610(config)# interface gigabitethernet 1/1` `DGS-3610(config-if)# spanning-tree link-type point-to-point`

Related commands

Command	Description
show spanning-tree interface	Show the STP port configuration.

17.1.5 spanning-tree max-hops

Use this global configuration command to set the number of max hops of the BPDU frame. The maximum-hop count is to specify the number of hops in a region before the BPDU is discarded, and it is valid for all instances. Use the **no** form of the command to restore 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 before the BPDU is discarded. The range is 1 to 40 hops.

Default configuration	The default is 20.
Command mode	Global configuration mode.
Usage guidelines	In the region, the BPDU sent by the root bridge includes a hot count. When a switch receives this BPDU, the hop count shall minus 1 until it decrements to 0. It shows the BPDU information is overtime. When the count reaches zero, the switch discards the BPDU. Changing the **max-hops** command affects all instances.

Examples

This example shows how to set the spanning-tree max-hops to 10 for all MST instances:

```
DGS-3610(config)# spanning-tree max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** privileged command.

Related commands

Command	Description
show spanning-tree	Shows the MSTP information.

17.1.6 spanning-tree mode

Use the stp version of this command in the global configuration mode. Use the **no** form of the command to restore the version of the spanning-tree to 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 configuration

MSTP version.

Command mode

Global configuration mode.

Examples

```
DGS-3610(config)# spanning-tree mode stp
```

Related commands

Command	Description
show spanning-tree	Show the spanning-tree configuration.

17.1.7 spanning-tree mst configure

Use this command to enter mst configuration mode in global configuration mode and configure the mstp region. Use the **no** form of the command to return all parameters (name, revision, and vlan map) to the default values.

spanning-tree mst configuration

no spanning-tree mst configuration

Default configuration	The default mapping is that all Vlans are mapped to the instance 0. The default name is an empty string. The revision number is 0.
Command mode	Global configuration mode.
Usage guidelines	To return to privileged mode, enter the **end** command or press **Ctrl+C**. To return to Global configuration mode, enter the **exit** command. After entering MST configuration mode, these configuration commands are available: **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to a MST instance. The range of instance-id is within the 0-64. Range of vlan is within 1-4095. vlan-range can indicate a set of VLANs, which shall be separated with comma. The consecutive VLAN numbers can be indicated in this way: 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. The default is that all the 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*]. (The range of instance is 1 to 64 with **no form**). **revision** *version*: Set the number of MST versions, within this range 0-65535. You can use the **no name** command to restore the default setting. **Show**: Displays the information of the MST region.

Examples	This example shows how to enter MST configuration mode, map VLANs 3. 5-10 to MST instance 1:
	`DGS-3610(config)# spanning-tree mst configuration`
	`DGS-3610(config-mst)# instance 1 vlan 3, 5-10`
	`DGS-3610(config-mst)# name region 1`
	`DGS-3610(config-mst)# revision 1`
	`DGS-3610(config-mst)# show`
	`MST configuration`
	`Name [region1]`
	`Revision 1`
	`Instance Vlans Mapped`
	`---------- --------------------`

```
0       1-2,4,11-4094
1       3,5-10
---------------------------------
DGS-3610(config-mst)# exit
DGS-3610(config)#
```

If you want to remove VLAN 3 from instance 1, you can execute this command after entering MST configuration mode:

```
DGS-3610(config-mst)# no instance 1 vlan 3
```

This example shows how to delete instance 1:

```
DGS-3610(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 an MST instance.
name	Configure the name of MST.
revision	Configure the revision of MST.
show	View the MST mode in the MST mode.

17.1.8 spanning-tree mst cost

Use this command to set the path cost for each instance in interface configuration mode. Use the **no** form of the command to restore the default setting.

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] *cost*

Parameter description

Parameter	Description
instance-id	The Instance ID, whose range is 0-64.
cost	Path cost is 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	Higher cost values represent higher costs.

Examples	This example shows how to set a path cost of 400 on a port associated with instances 3:
	`DGS-3610(config)# interface gigabitethernet 1/1`
	`DGS-3610(config-if)# spanning-tree mst 3 cost 400`
	You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Related commands

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 for an instance.

17.1.9 spanning-tree mst port-priority

Use this command to configure an interface priority for different instance in interface configuration mode. It will affect interfaces to put in the forwarding state when a loop occurs in region. Use the **no** form of the command to restore 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 number. Its range is 0–64.
priority	Interface priority, there are total 16 integer that are the multiple of 16. Priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.

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 higher priority interface will be put in the forwarding state. If all interfaces have the same priority value, the lowest interface number in the forwarding state.

Examples	This example shows how to set the priority of Gigabitethernet 1/1 to 10 in instance 20:
	`DGS-3610(config)# interface gigabitethernet 1/1`
	`DGS-3610(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 priority for different Instances.

17.1.10 spanning-tree mst priority

Use this command to set the equipment priority for the specified spanning-tree instance in global configuration mode. Use the **no** form of the command to restore the default setting.

spanning-tree [**mst** *instance-id*] **priority** *priority*

no spanning-tree [**mst** *instance-id*] **priority**

Parameter description

Parameter	Description
instance-id	Instance number. Its range is 0–64.
priority	Priority of the switch, which may be 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152,53248, 57344 and 61440. These 16 integers are all multiples of 4096.

Default configuration	The default instance-id is 0. The default of *priority* is 32768.

Command mode	Global configuration mode.
Examples	The following example sets the equipment priority of the Instance as 8192. `DGS-3610(config-if)# spanning-tree mst 20 priority 8192` You can verify your settings by entering the **show spanning-tree mst** instance **interface** *instance-id* privileged EXEC 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 port-priority	Set the port priority for an instance.

17.1.11 spanning-tree reset

Use this command to return the **spanning-tree** configuration to the default value. This command does not have the **no** form.

spanning-tree reset

Parameter description	None.
Command mode	Global configuration mode.
Examples	`DGS-3610(config)# spanning-tree reset`

Related commands

Command	Description
show spanning-tree	Show the STP global configuration.
show spanning-tree interface	Show the STP interface configuration.

17.1.12 spanning-tree tx-hold-count

Use this command to configure the TxHoldCount of the Global configuration STP, the maximum number of BPDUs sent in one second. Use the **no** form of the command to restore the default setting.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

Parameter description

Parameter	Description
tx-hold-count	Set the TxHoldCount. The range is from 1 to 10.

Default configuration

The default value is 3.

Command mode

Global configuration mode.

Examples

```
DGS-3610(config)# spanning-tree tx-hold-count 5
```

Related commands

Command	Description
show spanning-tree	Show the MSTP global configuration.

17.1.13 spanning-tree pathcost method

Use this command to configure the path cost of the port. Use the **no** form of the command to restore the default setting.

spanning-tree pathcost method [**long** | **short**]

no spanning-tree pathcost method

Parameter description

Parameter	Description
long	Adopt the 802.1t standard to configure path-cost values.
Short	Adopt the 802.1d standard to configure path-cost values.

Default configuration

By default, the 802.1T standard is used to set the value of Path-cost.

Command mode	Global configuration mode.

Examples

```
Switch(config-if)# spanning-tree pathcost method long
```

Related commands

Command	Description
show spanning-tree interface	Show the STP interface configuration.

17.1.14 spanning-tree portfast

Enable the portfast of the specified interface. You can use the **disabled** form of this command to disable the portfast feature of the interface.

spanning-tree portfast [**disabled**]

Parameter description

Parameter	Description
disabled	Disable the portfast of the interface.

Default configuration	Disabled.
Command mode	Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# spanning-tree portfast
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of an interface.

17.1.15 spanning-tree portfast bpduguard default

Open the BPDU 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	This command has no parameters.
Default configuration	BPDU guard is disabled.
Command mode	Global configuration mode.
Usage guidelines	If the BPDU is received from this port, the opened BPDU guard will enter the error-disabled status. Use the **show spanning-tree** command to display the configuration.
Examples	`DGS-3610(config)# spanning-tree portfast bpduguard default`

Related commands

Command	Description
show spanning-tree interface	Show the STP global configuration.

17.1.16 spanning-tree portfast bpdufilter default

Open the global BPDU filter. 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	This command has no parameters.
Default configuration	BPDU filter is disabled by default.
Command mode	Global configuration mode.
Usage guidelines	Corresponding port will not transmit or receive the BPDU after the BPDU filter is opened. Use the **show spanning-tree** command to display the configuration.

Examples	`DGS-3610(config)# spanning-tree portfast bpdufilter default`

Related commands	**Command**	**Description**
	show spanning-tree interface	Show the STP global configuration.

17.1.17 spanning-tree portfast default

Use this command to enable the portfast feature of all interfaces globally. Use the **no** form of the command to disable the portfast of all interfaces globally.

spanning-tree portfast default

no spanning-tree portfast default

Parameter description	This command has no parameters.
Default configuration	The portfast is disabled on all interfaces.
Command mode	Global configuration mode.
Examples	`DGS-3610(config)# spanning-tree portfast default`

Related commands	**Command**	**Description**
	show spanning-tree interface	Show the STP global configuration.

17.1.18 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	This command has no parameters.

Default configuration	Enabled.
Command mode	Global configuration mode.
Examples	`DGS-3610(config)# spanning-tree tc- protection`

17.1.19 spanning-tree tc-protection tc-guard

Enable the **tc-guard** switch globally. Use the **no** form of this command to disable the **tc-guard** switch globally. Enable the tc-guard function to prevent the spread of the tc message.

spanning-tree tc- protection tc-guard

no spanning-tree tc- protection tc-guard

Parameter description	There is no parameter in this command.
Default configuration	By default, the **tc-guard** switch is disabled.
Command mode	Global configuration mode.
Examples	`DGS-3610(config)# spanning-tree tc- protection tc-guard`

17.1.20 spanning-tree tc-guard

The interface enables the **tc-guard** switch. Use the **no** form of this command to disable the **tc-guard** switch. Enable the tc-guard function to prevent the tc message from spreading.

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter description	There is no parameter in this command.
Default configuration	By default, the **tc-guard** switch is disabled.

Command mode	Global configuration mode.

Examples

```
DGS-3610(config)# spanning-tree tc-guard
```

17.1.21 spanning-tree autoedge

Enable the Autoedge switch of some interface. User can use the **disabled** form of this command to disable the Autoedge switch of the interface.

spanning-tree autoedge [**disabled**]

Parameter description	The disabled is used to disable the **Autoedge** switch of the interface.
Default configuration	By default, it is enabled.
Command mode	Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# spanning-tree autoedge disabled
```

Related commands

Command	Function
show spanning-tree interface	Show the STP configuration information of a port.

17.1.22 bpdu src-mac-check

Enable the bpdu source mac check of some interface. Users can use the **no** form of this command to disable the bpdu source mac check function.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

Parameter description

Parameter	Description
H.H.H	Indicate to receive the source mac address as the bpdu frame of this address only.

	no	Indicate that the port receives any bpdu frames.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# bpdu src-mac-check 00d0.f800.1e2f
```

Related commands

None.

17.1.23 clear spanning-tree detected-protocols

Use this command to force the interface to send RSTP BPDUs and check the BPDUs.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter description

Parameter	Description
interface-id	ID of the interface.

Default configuration

None.

Command mode

Privileged mode.

Examples

```
DGS-3610(config)# clear spanning-tree detected-protocols
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the current interface.

17.2 Showing Related Command

17.2.1 show spanning-tree

Use this command to display the global spanning-tree configurations.

show spanning-tree [**summary** |**forward-time** | **hello-time** | **max-age** |

tx-hold-count | **pathcost** *method* | *max_hops*]

Parameter description

Parameter	Description
Summary:	Show information about each instance of MSTP and its port forwarding status.
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 mode.

Examples

DGS-3610# **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.

17.2.2 show spanning-tree interface

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 number.
bpdufilter	Show the status of bpdufilter .
portfast	Show the status of portfast.
bpduguard	Show the status of bpduguard.
link-type	Show the link type of an interface.

Command mode

Privileged mode.

Examples

```
DGS-3610#  show spanning-tree interface gigabitethernet 1/5
```

Related commands

Command	Description
spanning-tree bpdufilter	Enable the BPDU filter feature of some interface.
spanning-tree portfast	Enable the portfast for an interface.
spanning-tree bpduguard	Enable the BPDU guard for an interface.
spanning-tree link-type	Set the link type of an interface to “point-to-point".

17.2.3 show spanning-tree mst

In privileged mode, use this command to display the information of MST and instance.

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

Show all the instances.

configuration

Command mode

Privileged mode.

Examples

```
DGS-3610# 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 an instance.
spanning-tree mst max-hops	Show the maximum hops of an instance.
spanning-tree mst priority	Show the equipment priority of instance.
spanning-tree mst port-priority	Show the port priority of an instance.

18 Configuring SPAN command

18.1 monitor session

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. For *interface-id*, assign the interface identifier, it should be physical interface, neither AP nor SVI.
destination interface *interface-id*	Specify the destination port. For interface-id, specify the related interface number; it can be only for a physical interface, not SVI or AP interface.
mac source *mac-addr*	Source MAC of the mirrored frame
mac destination *mac-addr*	Destination MAC of the mirrored frame
Both **acl** *name*	Monitor both input and output frames. **acl** *name/id* of monitored flow
rx	Monitor input frames.
tx	Monitor output frames.
all	Delete all sessions
encapsulation	Support encapsulation function of mirrored port.

	Once enable it, the message tag will be forcely removed . It's disabled by default
switch	Support mirror destination port switching function. 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 has no effect on the normal operation of the equipment. You can configure a SPAN session on disabled ports. However, SPAN does not become active 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.

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 the port 1 to the port 8.

```
DGS-3610(config)# no monitor session 1
DGS-3610(config)# monitor session 1 source interface
gigabitEthernet 1/1 both
DGS-3610(config)# monitor session 1 destination
interface gigabitEthernet 1/8
```

Related commands

Command	Description
show monitor	Use this command to display the SPAN configurations.

18.2 Show monitor

Use this command to display the SPAN configurations.

show monitor [**session** *session_number*]

Default

All SPAN sessions are displayed by default.

configuration

Parameter description

Parameter	Description
session *session_number*	SPAN session number.

Command mode

Privileged mode.

Usage guidelines

None.

Examples

This example shows how to use **show monitor** to display SPAN session 1**:**

```
DGS-3610# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

Related commands

Command	Description
monitor session	Specify a SPAN session and the destination port and the source port.

19 Configuring IP Address Commands

19.1 Interface Address Configuration Commands

The interface address configuration include the commands as follows:

- **ip-address**
- **ip unnumbered**

19.1.1 ip-address

This command is used to configure the IP address of interface. The **no** form can be used to delete the IP address of a specified interface. The command format is as follows:

ip address *ip-address network-mask* [**secondary**]

no ip address *ip-address network-mask* [**secondary**]

Parameter description

Parameter	Description
ip-address	32-bit IP address, 8 bits in one group, in decimal. Groups are separated by dots.
network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit. 8 bits in one group, in decimal. Groups are separated by dots.
secondary	Indicate the secondary IP address that has been configured.

Default The interface is not equipped with IP address.

Usage guidelines Interface configuration mode.

Usage guidelines The equipment cannot receive and send IP packets before 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 for class A network 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.

DGS-3610 series 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 can be configured. The secondary IP address and the primary IP address can 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 router should be connected to two networks and multiple IP addresses should be configured.
- Many older networks are the second layer-based bridge network that has 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 router 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 connected the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces in the router.

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
```

Related commands

Command	Description
show interface	Show detailed information of the interface.

Platform description

On a layer 2 switch, an IP address can be configured for layer 3 interfaces only, and layer 2 addresses are not supported, namely there is no **secondary** option.

19.1.2 ip unnumbered

This command is used to configure an unnumbered interface. After an interface is configured as unnumbered interface, it is allowed to run the IP and can receive and send IP packets. The **no** form can be used to cancel this configuration.

ip unnumbered *interface-type interface-number*

no ip unnumbered *interface-type interface-number*

Parameter description

Parameter	Description
interface-type	Associate interface type
interface-number	Associate interface number

Default

By default, no unnumbered interface is configured.

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 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 0/0. An IP address must be configured for the associated interface.

```
ip unnumbered fastEthernet 0/0
```

Related commands

Command	Description
show interface	Show detailed information of the interface.

Platform description

The command is supported by the L2 equipments.

19.2 Address Resolution Protocol (ARP) Configuration Commands

The address resolution protocol (ARP) configuration commands include as follows:

- **arp**
- **arp retry**
- **arp trusted**
- **arp unresolved**
- **arp gratuitous-send**
- **arp timeout**
- **ip agent-arp**
- **service trustedarp**

19.2.1 arp

This command allows you to add a permanent IP address and MAC address mapping to the ARP cache table. The **no** form of this command is used to delete 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. Different parts are separated by dots.
MAC-address	Data link layer address that contains 48 bits.
type	ARP encapsulation type. The keyword is **arpa** for the Ethernet interface.
alias	(Optional) DGS-3610 series 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

DGS-3610 series 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 learnt dynamically.

Examples

The following example sets an ARP static mapping record for a host in the Ethernet.

```
arp 1.1.1.1 4e54.3800.0002 arpa
```

Related commands

Command	Description
clear arp-cache	Clear the ARP cache table

19.2.2 arp retry interval

This command is used to set the frequency for sending the arp request message locally, namely, the time interval between two continuous sent ARP requests for the resolution of the same IP address. The **no** form of this command is used to restore the default retry of 1 ARP request per second.

arp retry interval *seconds*

no arp retry interval

Parameter description

Parameter	Description
seconds	<1-3600>, the retry time of the ARP request can be set as 1 – 3600s, 1s by default.

Default configuration

The retry interval of the ARP request is 1s.

Command mode

Global configuration mode.

Usage guidelines

When it is discovered that this device sends out the ARP request frequently and causes other problems such as the busying of the network, the retry interval of the ARP request can be set as longer. In general, it should not exceed the aging time of the dynamic ARP item.

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.

19.2.3 arp retry times

This command can be used to set the local retry times of the arp request message, namely, the times of the continuous sent ARP request for the resolution of the same 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 sending times of the same ARP request, with the range <1-100>. 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 timeout.
Command mode	Global configuration mode.
Usage guidelines	When it is discovered that this device sends out the ARP request frequently and causes other problems such as the busying of the network, the retry times of the ARP request can be set as smaller. In general, the retry times should not be set too large.

Examples	The following configuration disables transmission retry of the local ARP request.
	`arp retry times 1`
	The following configuration 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.

19.2.4 arp trusted

This command can be used set the maximal quantity of the trusted ARP item.The **no** form of this command is restored to the default value.

arp trusted *number*

no arp trusted

Parameter description

Parameter	Description
number	Can set the maximal quantity of the trusted ARP item, with the range <10-4096>.

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 item and other items share the memory. If the trusted items are occupied too much, it may result in there is no enough dynamic ARP items. In general, it is set on demand, and the value should not be set too much.
Examples	The following configuration can set 1000 trusted ARPs. `arp trusted 1000`

Related commands

Command	Function
service trustedarp	Enable the trusted ARP function.

19.2.5 arp unresolve

This command can be used to configure the maximal quantity of the unresolved item in the ARP items.The **no** form of this command can restore the default value 8192.

arp unresolve *number*

no arp unresolve

Parameter description

Parameter	Description
number	The maximal quantity of the unresolved ARP item, with the range <1-8192>.The default value is 8192.

Default configuration	The ARP buffer table can contain up to 8192 resolution items.
Command mode	Global configuration mode.
Usage guidelines	If it is discovered that there is a large number of the unresolved items in the RP buffer table and it is not disappeared after a period of time, this command can be used to limit the quantity of the unresolved items.

Examples	The following configuration sets the maximal quantity of the unresolved items as 500. `arp unresolved 500`
Related commands	None

19.2.6 arp gratuitous-send interval

This command can be used to send the free ARP request at the specified network interface regularly. 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 (unit: second), with the range <1-3600>.

Default configuration	This interface doesn't enable the function to send the free ARP request regularly.
Command mode	Interface configuration mode.
Usage guidelines	If the network interface of the devices is taken as the gateway of the downlink devices, and there is the counterfeit gateway behavior in the downlink devices, it can configure to send the free ARP request regularly on this interface, to notify that it is the true gateway.

Examples

The following configuration sets to send one free ARP request to SVI 1 per second.

```
DGS-3610(config)# interface vlan 1
DGS-3610(config-if)# arp gratuitous-send interval 1
```

The following configuration stops sending the free ARP request to SVI 1.

```
DGS-3610(config)# interface vlan 1
DGS-3610(config-if)# no arp gratuitous-send
```

Related commands

None

19.2.7 arp timeout

This command can be used to configure the timeout for the ARP static mapping record in the ARP cache. The **no** form of this command is used to restore the default configuration.

arp timeout *seconds*

no arp timeout

Parameter description

Parameter	Description
seconds	The timeout, in seconds, ranging 0-2147483

Default

The default timeout is 3600 seconds.

Command mode

Global configuration mode.

Usage guidelines

The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learnt 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 example sets the timeout for the dynamic ARP mapping record that is learnt dynamically from FastEthernet 0/0 to 120 seconds.
	`interface fastEthernet 0/0`
	`arp timeout 120`

Related Command	

19.2.8 ip proxy-arp

Execute the ip proxy-arp command to enable the function of agent ARP. The no form of this command can disable the function of agent ARP.

ip proxy-arp

no ip proxy-arp

Default Setting	Enable the agent ARP by default.
Command mode	Interface configuration mode.
Usage guidelines	The proxy ARP function of a device helps a host without any routing information obtain IP addresses and MAC addresses of other networks or subnets. For example, a device receives an ARP request. The ARP request sender's IP address and the requested IP address belong to different networks, and the device knows the route to the requested IP address, and it sends an ARP response. The responded MAC address is the Ethernet MAC address of the device itself. The above process is the function of proxy ARP.

Examples	Following configuration is to enable the function of agent ARP on the FastEthernet 0.
	`interface fastEthernet 0`
	`ip proxy-arp`

Platform Description	This command is not supported on L2 devices.

19.2.9 service trustedarp

To enable the trusted ARP function, you can execute the **service trustedarp** command. The **no** form of this command disables the trusted ARP function.

service trustedarp

no service trustedarp

Default configuration	Disable the trusted ARP by default.
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.

Examples	The following configuration is to enable the service trustedarp function in the global configuration mode.
	`config`
	`service trustedarp`

Platform description	This command is not supported on L2 devices and s32.

19.3 IP Route Configuration Commands

19.3.1 ip route

To configure a static route, use the global configuration command **ip route**. The **no** form of this command is used to delete a static route that has been configured.

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	VRF_name
network	Network number of the default network.

net-mask	Network mask of the static route
ip-address	Next hop address of the static route
interface	(Optional) Next hop exit of the static route
distance	(Optional) Administrative distance of the static route
tag	(Optional) Tag value of the static route
permanent	(Optional) Permanent route identifier
number	(Optional) Weight value of the static route
disable/enable	(Optional) Enable identifier of the static route

Default configuration

There is no static route by default.

Command mode

Global configuration mode.

Usage guidelines

The default administrative distance for the static route is 1. Setting an administrative distance will allow the dynamically learnt route to overwrite the dynamic route. A static route is used only when it is unable to learn the dynamic route. The line can be backed up by setting an administrative distance for the static route. In this case, the static route is also called floating route. For example, the administrative distance of the OSPF routing protocol is 110. The administrative distance for the static route can be set as 125. In this way, when the line that runs OSPF fails, the data flow will be switched over to the line of static route.

It can specify the vrf the static route is of. Add it to the default vrf if it is not specified.

The enable flag of the static route controls whether the static route is effective. It will not be used for forwarding if not effective. A permanent route is configured into the forwarding table and will always exist unless removed by the network administrator.

Please avoid using the next hop (ip route 0.0.0.0 0.0.0.0 fastethernet 0/0) as the interface when you want to configure a static route through the Ethernet interface. Otherwise, the router will think that all the unknown destination networks are directly connected to the

	fastethernet 0/0 interface, and will send an ARP request to every destination host. This will occupy a large number of CPU and memory resources. Therefore, it is not recommended to direct a static route to an Ethernet interface.

Examples	The following example adds a static route to the destination network 172.16.100.0/24, with the next hop address 192.168.12.1 and the administrative distance as 115.
	`ip route 172.16.100.0 255.255.255.0 192.168.12.1 115`
	If no interface is specified for the static route, the data flow may be sent from other interfaces when the interface that is often used fails. An interface should be specified in order to avoid this. The following example specifies that the data flow to the destination network 172.16.100.0/24 can be forwarded through the fastethernet 0/0 interface only.
	`ip route 172.16.100.0 255.255.255.0 fastethernet 0/0 192.168.12.1`

Related commands

Command	Description
show ip route	Show the IP routing table

Platform description	The command is supported by the L2 equipments.

19.3.2 ip default-network

To configure a default network, use the global configuration command **ip default-network**. The **no** form of this command is used to delete the default network.

ip default-network *network*

no ip default-network *network*

Parameter description

Parameter	Description
network	Network number of the default network.

Default configuration	The default is 0.0.0.0/0.
Command mode	Global configuration mode.
Usage	The purpose of configuring a default network is to generate a default

guidelines	network. To generate a default route using default-network, the default network should not be a directly connected network, but should be reachable in the routing table. The default network always starts with "*", which indicates that it is the candidate of the default route. If there are connected route and routes without next hop in the default network, the static route should be used as the default route.

Examples	The following example sets the 192.168.100.0 network as the default network. The router will automatically produce a default route since a static route to this network has been configured.
	`ip route 192.168.100.0 255.255.255.0 serial 0/1`
	`ip default-network 192.168.100.0`
	The configuration example below sets the network 200.200.200.0 as the default network. Once 200.200.200.0 shows in the routing table, this route will become the default route.
	`ip default-network 200.200.200.0`

Related commands

Command	Description
show ip route	Show the IP routing table

Platform description	The command is supported by the L2 equipments.

19.3.3 ip routing

To enable the IP routing function of DGS-3610 series, execute this command in the global mode. The **no** form of this command is used to disable the IP routing function.

ip routing

no ip routing

Default	The IP routing is enabled.

Command mode	Global configuration mode.

Usage guidelines	The IP route forwarding function of DGS-3610 series is useless when the router is only used as a bridge device or as a VOIP gateway device. In this case, the IP routing function of DGS-3610 series can be disabled.

Examples

The example below shows how to disable the IP routing function of DGS-3610 series.

```
no ip routing
```

Platform description

The command is supported by the L2 equipments.

19.3.4 maximum-paths

To configure the number of equivalent routes, use the global configuration command **maximum-paths**. The **no** form of this command is used to reset the default number of equivalent routes.

maximum-paths *number*

no maximum-paths *number*

Parameter description

Parameter	Description
number	Number of equivalent routes, ranging 1-32

Default configuration

The default value is 32.

Command mode

Global configuration mode.

Usage guidelines

The purpose of configuring the number of equivalent routes is to control the number of equivalent routes. After this number is configured using **maximum-paths**, the number of paths for load balancing will not exceed the configured number of equivalent routes. The **show running config** command is used to show the number of equivalent routes.

Examples

The following example sets the maximum number of equivalent routes to 10 and then resets the default value.

```
maximum-paths 10
no maximum-paths
```

Platform description

The command is supported by the L2 equipments.

19.3.5 ip static route-limit

To configure the upper limit of the static routes, use the global configuration command **ip static route-limit**. The **no** form of this command is used to reset the default number of equivalent routes.

ip static route-limit *number*

no ip static route-limit *number*

Parameter description

Parameter	Description
number	The upper limit. The range is 1-10000.

Default configuration

The default value is 1000.

Command mode

Global configuration mode.

Usage guidelines

The purpose to configure the upper limit of static routes is to control the quantity of static routes. The configured static routes will not exceed the upper limit of the setting when it is set by the **ip static route-limit.** The upper limit of current configured non-default static routes can be viewed by the **show running config** command**.**

Examples

The configuration example below sets the upper limit of the static routes as 900, and then restores it to the default value.

```
ip static route-limit 900
```

Platform description

The command is supported by the L2 equipments.

19.4 Broadcast Message Processing Configuration Commands

The broadcast message processing configuration related commands include:

- **ip broadcast-addresss**
- **ip directed-broadcast**

19.4.1 ip broadcast-addresss

To define a broadcast address for an interface, use the interface configuration command **ip broadcast-addresss**. The **no** form of this command is used to cancel the broadcast address configuration.

ip broadcast-addresss *ip-address*

no ip broadcast-addresss *ip-address*

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 DGS-3610 series 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 example sets 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

The command is supported by the L2 devices.

19.4.2 ip directed-broadcast

To enable the conversion from directed broadcast of IP to physical broadcast, use the interface configuration command **ip directed-broadcast**. The **no** form of this command is used to cancel the conversion from directed broadcast to physical broadcast.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter description

Parameter	Description
access-list-number	(Optional) Access list number, ranging 1-199 and 1300 – 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 router 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 router that is directly connected to this subnet, the router 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, DGS-3610 series will discard the directed broadcast packets received for the directly connected network.

Examples

The following example enables forwarding of directed broadcast packet on the fastEthernet 0/0 port of a router.

```
interface fastEthernet 0
ip directed-broadcast
```

Platform description	The command is supported by the L2 equipments.

19.5 IP Address Monitoring and Maintenance Commands

The IP address monitoring and maintenance related commands include:

- **clear arp-cache**
- **show arp**
- **show arp counter**
- **show arp timeout**
- **clear ip route**
- **show ip arp**
- **show ip interface**

19.5.1 clear arp-cache

To remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table, use the global command **clear arp-cache**.

clear arp-cache [*A.B.C.D*] | **interface** *interface-name*]

Command mode	Privileged mode.
Usage guidelines	This command can be used to refresh an ARP cache table.

Examples	The following example removes all dynamic ARP mapping record.
	`clear arp-cache`
	The following example removes dynamic ARP table entry 1.1.1.1
	`clear arp-cache 1.1.1.1`
	The following example removes 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 table.

19.5.2 show arp

Show the Address Resolution Protocol (ARP) cache table

show arp *[ip [mask]* | *mac-address]* | **static | complete | incomplete**

Parameter description

Parameter	Description
ip	ip address, shows the specified ARP entry of ip address
ip mask	Show the ARP entry of the network segment included within ip mask
mac-address	Show the ARP entry of specified mac address
static	Show all the static arp entries
complete	Show all the dynamic arp entries resoluted.
incomplete	Show all the dynamic arp entries not resoluted

Command mode

No requirement.

Examples

The following is the output result of the show ip arp command:

```
DGS-3610# 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:

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*

```
DGS-3610# 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*

```
DGS-3610# 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*

```
DGS-3610# 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	This command is not supported on the L2 devices.

19.5.3 show arp counter

This command shows the number of arp entries in the ARP buffer table.

show arp counter

Parameter description	None.
Command	No requirement.

mode	

Examples	The following is the output result of the **show arp counter** command:
	`DGS-3610# 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 as below:

Platform description	This command is not supported on the L2 devices.

19.5.4 show arp timeout

This command shows the aging time of the dynamic ARP entries on a port.

show arp timeout

Parameter description	None.
Command mode	No requirement.

Examples	The following is the output result of the **show arp timeout** command:
	`DGS-3610# show arp timeout`
	`Interface arp timeout(sec)`
	`---------- ----------`
	`VLAN 1 3600`
	The meaning of each field in the ARP cache table is described as below

Platform description	This command is not supported on the L2 devices.

19.5.5 clear ip route

To refresh the entire IP routing table or a particular routing record in the IP routing table, execute the **clear ip route** command 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 routes for 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

The command is supported by the L2 equipments.

19.5.6 show ip arp

To show the Address Resolution Protocol (ARP) cache table, execute this command in the privileged user mode.

show ip arp

Parameter description

None.

Command mode

Privileged mode.

Examples

Presented below is the output of **show ip arp**:

```
DGS-3610# 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	Protocol for network address. This filed is always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Duration in which the ARP cache record exists, in minutes. For local or static configuration, the value of this field is represented by "-".
Hardware	Hardware address corresponding to the IP address.
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

Platform description

The command is supported by the L2 equipments.

19.5.7 show ip interface

This command shows the IP status information of an interface. The command format is as follows:

show ip interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Specify interface type
interface-number	Specify interface number

Command mode

Privileged mode.

Usage guidelines

When an interface is available, DGS-3610 series will create a direct route in the routing table. The interface is available in that DGS-3610 series can receive and send packets through this interface. If the interface changes from available status to unavailable status, DGS-3610 series remove 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**:

```
DGS-3610# show ip interface
FastEthernet 0/0
IP interface state is: UP
IP interface type is: BROADCAST
IP interface metric is: 0
IP interface MTU is: 1500
IP address is:
192.168.5.133/24 (primary)
IP address negotiate is: OFF
Forward direct-boardcast is: ON
ICMP mask reply is: ON
Send ICMP redirect is: ON
Send ICMP unreachabled is: ON
DHCP relay is: OFF
Fast switch is: ON
Route horizontal-split is: ON
Help address is: 0.0.0.0
Agent ARP is: ON
Outgoing access list is not set.
Inbound access list is not set.
```

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.**
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.**

19.5.8 show ip redirects

Use this command to display the default gateway. The command format is as below:

show ip redirects

Parameter description	None.
Command mode	Privileged mode.
Usage	This command is only supported on the L2 device.

guidelines

Examples

The following is the output result of the **show ip redirects**:

```
DGS-3610# show ip redirects

Default Gateway: 192.168.195.1
```

20 Configuring IP Service Configuration Commands

20.1 IP Service Configuration Commands

The IP service configuration related commands include:

- **ip mask-reply**
- **ip mtu**
- **ip redirects**
- **ip source-route**
- **ip unreachables**

20.1.1 ip mask-reply

In order for DGS-3610 series to respond to the request for ICMP mask request and send an ICMP response message, use the interface configuration command **ip mask-reply**. The **no** form of this command is used to prohibit from sending an ICMP mask response message.

ip mask-reply

no ip mask-reply

Default	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 example sets the FastEthernet 0/0 interface of a router to respond the ICMP mask request message.

```
interface fastEthernet 0/0
ip mask-reply
```

Platform description

The command is supported by the L2 equipments.

20.1.2 ip mtu

To set the Maximum Transmission Unit (MTU) for an IP packet, use the interface configuration command **ip mtu**. The **no** form of this command is used to restore the default configuration.

ip mtu *bytes*

no ip mtu

Parameter description

Parameter	Description
bytes	Maximum transmission unit of IP packet, in bytes, ranging 68~1500.

Default

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, DGS-3610 series 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 example sets the IP MTU value of the fastEthernet 0/0 interface to 512 bytes.

```
interface fastEthernet 0/0
ip mtu 512
```

Related commands	**Command**	**Description**
	mtu	Set the MTU value of an interface.

Platform description	The command is supported by the L2 equipments.

20.1.3 ip redirects

To allow DGS-3610 series to send an ICMP redirection message, use the interface configuration command **ip redirects**. The **no** form of this command is used to disable the ICMP redirection function.

ip redirects

no ip redirects

Default	It is enabled by default.
Command mode	Interface configuration mode.
Usage guidelines	When the route is not optimum, it may make the router to receive packets through one interface and send it though the same interface. If the router sends the packet through the interface through which this packet is received, the router will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another router in the subnet. This way the data source will send subsequent packets along the optimum path. DGS-3610 series enables ICMP redirection by default.

Examples	The following example disables ICMP redirection for the fastEthernet 0/0 interface.
	`interface fastEthernet 0/0`
	`no ip redirects`

Related commands	**Command**	**Description**
	show ip redirects	Show the default gateway and ohly supported on L2 devices.

Platform description	The command is supported by the L2 equipments.

20.1.4 ip source-route

To allow DGS-3610 series to process an IP packet with source route information, use the global configuration command **ip source-route**. The **no** form of this command is used to disable the source route information processing function.

ip source-route

no ip source-route

Default	It is enabled by default.
Command mode	Global configuration mode.
Usage guidelines	DGS-3610 SERIES supports IP source route. When the router 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 have been 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. DGS-3610 series supports IP source route characteristic by default.
Examples	The following example disables the IP source route characteristic. `no ip source-route`
Platform description	The command is supported by the L2 equipments.

20.1.5 ip unreachables

To allow DGS-3610 series to generate an ICMP destination unreachable message, use the interface configuration command **ip unreachables**. The **no** form of this command is used to prohibit from sending an ICMP destination unreachable message.

ip unreachables

no ip unreachables

Default	It is enabled by default.

Command mode	Interface configuration mode.
Usage guidelines	If DGS-3610 series receives a unicast message with its own destination address but is unable to the upper-layer protocol of this message, it will send an ICMP destination unreachable message. If DGS-3610 series fails to forward a packet due to lack of routes, it will send an ICMP host unreachable message to the data source. This command affects all the ICMP destination unreachable messages.

Examples	The following example disables sending of ICMP destination unreachable message through the fastEthernet 0/0 interface.
	`interface fastEthernet 0/0`
	`no ip unreachables`

Platform description	The command is supported by the L2 equipments.

21 Configuring DHCP Command

21.1 DHCP Configuration Related Command

DHCP configuration includes the following commands:

- **bootfile**
- **client-identifier**
- **client-name**
- **default-router**
- **dns-server**
- **domain-name**
- **hardware-address**
- **host**
- **ip address dhcp**
- **ip dhcp excluded-address**
- **ip dhcp ping packet**
- **ip dhcp ping timeout**
- **ip dhcp pool**
- **lease**
- **netbios-name-server**
- **netbios-node-type**
- **network (DHCP)**
- **next-server**
- **option**
- **service dhcp**

21.1.1 bootfile

To define the startup mapping file name of DHCP client, use the DHCP address pool configuration command **bootfile**.The **no** form of this command can be used to cancel the definition.

bootfile *file-name*

no bootfile

Parameter description

Parameter	Description
file-name	Define the 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, so DHCP server should provide the mapping file name required for the startup, so that DHCP client can download the file by corresponding server (such as TFTP).Other servers are defined by the **next-server** command.

Examples

The configuration example below defines the router.conf as the startup file name.

```
bootfile router.conf
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.
next-server	Configure the next server IP address of the DHCP client startup process.

21.1.2 client-identifier

To define the unique ID of the DHCP client (indicated in hex, separated by dot), use the DHCP address pool configuration command **client-identifier**. 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.Such as: 0100.d0f8.2233.b467.6967.6162.6974.4574.6865. 726e.6574.302f.31.

Default

No default value.

Command mode

DHCP address pool configuration mode.

Usage guidelines

When some DHCP clients request the DHCP server to assign the IP address, use the client ID to denote the client, instead of the hardware address. The client ID consists of the type of medium, MAC address and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and 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 medium.

The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is

The hex code of GigabitEthernet0/1. For the definition of the medium 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.Used to configure the DHCP manual binding.
ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.

21.1.3 client-name

To define the name of the DHCP client, use the DHPC address pool configuration command **client-name**. 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	Define the name of DHCP client. The ASCII character set of any standards can be used. 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 by default.

Command mode DHCP address pool configuration mode.

Usage guidelines This command can be used to define the name of 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. Used to configure the DHCP manual binding.
ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.

21.1.4 default-router

To define the default gateway of the DHCP client, use the DHPC address pool configuration command **default-router**.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 default 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 configuration mode of the DHCP address pool.

21.1.5 dns-server

To define the DNS server of the DHCP client, use the DHPC address pool configuration command **dns-server**.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 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 learnt by the DHCP client of DGS-3610 series 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 DGS-3610 series 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 DHCP client.
	ip address dhcp	The interface enables the DHCP client to obtain the IP address information.
	ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.

21.1.6 domain-name

To define the suffix domain name of the DHCP client, use the DHPC address pool command **domain-name**.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 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 the 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 DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.

21.1.7 hardware-address

To define the hardware address of the DHCP client, use the DHPC address pool configuration command **hardware-address**.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 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, 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 DHCP client (Indicated by the hexadecimal numeral, separated by dot).
host	Define the IP address and network mask.Used to configure the DHCP manual binding.
ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.

21.1.8 host

To define the IP address and network mask of the DHCP client host, use the DHCP address pool configuration command **host**.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.

host *ip-address* [*netmask*]

no host

Parameter description

Parameter	Description
ip-address	Define the IP address of DHCP client host.
netmask	Define the network mask of DHCP client host.

Default	The IP address or network mask of the host is not 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: The network mask for the class A address is 255.0.0.0, that for the class B address is 255.255.0, and it is 255.255.255.0 for the class C 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 should prevent to be 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 configuration mode of the DHCP address pool.

21.1.9 ip address dhcp

To make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP, use the interface configuration command **ip address dhcp**.The **no** form of this command can be used to cancel this configuration.

ip address dhcp

no ip address dhcp

Default	The interface can not 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 DGS-3610 series 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 DNC server information, 4) DHCP option 15, the host suffix domain name, DHCP option 44, the WINS server information.

The client of DGS-3610 series allows obtaining the address on the PPP, FR or HDL link by the dhcp, which should be supported by the server. At present, out 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 configuration mode of the DHCP address pool.

21.1.10 ip dhcp excluded-address

To define some IP addresses and make the DHCP server not assign them to the DHCP client, use the global configuration command **ip dhcp excluded-address**.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 address 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. 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 the configuration mode of the DHCP address pool.
network (DHCP)	Define the network number and network mask of the DHCP address pool.

21.1.11 ip dhcp ping packet

To configure the DHCP server to detect the address conflict and ping the times of this address, use the global configuration command **ip dhcp ping packet**. The no form of this command is used to restore default configuration.

ip dhcp ping packet [*number*]

no ip dhcp ping packet

Parameter description

Parameter	Description
number	(Optional) the range changes from 0 to 10, where, 0 indicates to close the ping operation. Ping two packets by default.

Default	Ping 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 two data packets by default, up to 10 packets at most.
Examples	The configuration example below sets the quantity 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 of the waiting for response for the DHCP server ping operation. All ping packets are not responded within specified time. It indicates that this address can be assigned. Otherwise, it will record the address conflict.
show ip dhcp conflict	Show the DHCP server detects the address conflict when it assigns the address.

21.1.12 ip dhcp ping timeout

To configure the timeout of waiting for response when the DHCP server uses the ping operation to detect the address conflict, use the global configuration command **ip dhcp ping timeout**. The **no** form of this command can be used to restore the default configuration.

ip dhcp ping timeout *milli-seconds*

no ip dhcp ping timeout

Parameter description

Parameter	Description
milli-seconds	The time when the DHCP server waits the ping response (in ms). The range of the value is 100 – 1000.

Default	The default timeout is 500 seconds.
Command mode	Global configuration mode.

Usage guidelines	Define the time used to wait 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 quantity of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns the address.
show ip dhcp conflict	Show the DHCP server detects the address conflict when it assigns the address.

21.1.13 ip dhcp pool

To define a name of the DHCP address pool and enter into the configuration mode of the DHCP address pool, use the global configuration command **ip dhcp pool**.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	Can consist of the characters and positive integers.Such as mypool or 1.

Default	No DHCP address pool is defined, by default.
Command mode	Global configuration mode.
Usage guidelines	Execute the command to enter the DHCP address pool configuration mode, as is sown below: `DGS-3610(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.Used to configure the DHCP manual binding.
ip dhcp excluded-address	Define the IP addresses that the DHCP server can not assign to the client.
network (DHCP)	Define the network number and network mask of the DHCP address pool.

21.1.14 lease

To define the lease time the DHCP server assigns to the client address, use the DHCP address pool configuration command **lease**. The **no** form of this command can be used to restore default configuration.

lease { *days* [*hours*] [*minutes*] | **infinite** }

no lease

Parameter description

Parameter	Description
days	Define the lease time, taking days as the unit.
hours	(Optional) Define the lease time, taking hours as the unit. It is necessary to define the days before you define the hours.
minutes	(Optional) Define the lease time, taking minutes as the unit. It is necessary to define the days and hours before you define the minutes.
infinite	Define the infinite lease.

Default

The lease is 1 days by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

When the lease is near to expire, the DHCP client will send the request to continue to release. In general, the DHCP server will allow the lease, and the address of the lease will keep constant.

Examples

The configuration example below sets the DHCP lease as 1 hour.

```
lease 0 1
```

The configuration example below sets the DHCP lease as 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 configuration mode of the DHCP address pool.

21.1.15 netbios-name-server

To configure the WINS name server of the Microsoft DHCP client NETBIOS, use the DHCP address pool configuration command **netbios-name-server**. 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	Define the IP address of the WINS server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) 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 will possess higher priory, so 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 commands

Command	Description
ip address dhcp	The interface enables the DHCP client to obtain the IP address information.

	ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.

21.1.16 netbios-node-type

To define the type of nodes for the Microsoft DHCP client master NetBIOS, use the DHCP address configuration **netbios-node-type**. The **no** form of this command can be used to delete the configuration of the NetBIOS node types.

netbios-node-type *type*

no netbios-node-type

Parameter description

Parameter	Description
type	Define the type of the NetBIOS node in two ways. The definition in digits with the range of 0~FF in hexadecimal number, but only the value below can be obtained: ■ 1, denotes b-node. ■ 2, denotes p-node. ■ 4, denotes m-node. ■ 8, denotes h-node. The Definition in String: ■ b-node, the type of the broadcast node. ■ p-node, the type of the peer-to-peer node. ■ m-node, the type of the mixed node. ■ h-node, the type of the 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 Microsoft DHCP client NetBIOS nodes: 1) Broadcast, the type of the broadcast node, which carry out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, the type of the peer-to-peer node, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, the type of the mixed node, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, the type of the hybrid node, 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 type of the nodes for Microsoft operating system is of the broadcast or hybrid. If the WINS server is not configured, it is of the broadcast node. Otherwise, if the WINS server is configured, it is of the hybrid node. 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 configuration mode of the DHCP address pool.
netbios-name-server	Configure the WINS name server of the Microsoft DHCP client NETBIOS.

21.1.17 network (DHCP)

To define the network number and network mask of the DHCP address pool, use the DHCP address pool configuration command **network**. 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	The IP address network number of the DHCP address pool

	net-mask	The IP address network mask of the DHCP address pool. If the network mask is not defined, it will be the natural network mask, by default.

Default	No network number or network mask is defined by default.
Command mode	DHCP address pool configuration mode.
Usage guidelines	Define the subnet and subnet mask of new address pool, and provide the DHCP server with an address space which can be assigned to the client. Unless there are collided configured in the addresses, the address of all address pools can be assigned to the client. The DHCP assigns the addresses in the address pool in the sequence, if this address is in the DHCP binding table of this address is detected to exist in this network segment, check this address until an effective address is assigned. 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 detection conflict.
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 can not assign to the client.
	ip dhcp pool	Define the name of the DHCP address pool and enter into the configuration mode of the DHCP address pool.

21.1.18 next-server

To define the startup sever list to be accessed during the DHCP client startup, use the DHCP address configuration command **next-server**.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 There is no default configuration.

Command mode DHCP address pool configuration mode.

Usage guidelines When more than one startup server is defined, the former will possess higher priory, so 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 configuration mode of the DHCP address pool.
ip help-address	The interface defines the Helper address.
option	Configure the option of DGS-3610 series DHCP server.

21.1.19 option

To configure the option of the DHCP server, use the DHCP address pool configuration command **option**.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 the hex string.
ip *ip-address*	Define the IP address list.

Default

No default configuration.

Command mode

Global configuration mode.

Usage guidelines

The DHCP provides a mechanism to allow transmit the configuration information to the host by the TCP/IP network. The DHCP message is assigned an option field especially, this part of content of the variable one and 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 makes the DHCP client enable the IP packet forwarding.

```
option 19 hex 1
```

The configuration example below defines the option code 33, which provides the DHCP client with the static route information, and 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 the configuration mode of the DHCP address pool.

21.1.20 service dhcp

To enable the DHCP server and relay agent characteristic in the equipment, use the global configuration command **service dhcp**. The **no** form of this command can be used to disable the DHCP server and relay agent characteristic.

service dhcp

no service dhcp

Parameter description	None.
Default	Enable the DHCP server and relay agent characteristic, by default.
Command mode	Global configuration mode.
Usage guidelines	The DHCP server can assign the IP address to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP agent feature can forward DHCP requests to other servers, and forwards the returned DHCP response packets to the DHCP client, serving as the relay for DHCP packets.
Examples	In the following configuration example, the router has enabled the DHCP server and trunk feature. `service dhcp`

Related commands

Command	Description
show ip dhcp server statistics	Show various statistics information of the DHCP server.

21.2 Showing and Monitoring Commands

- **clear ip dhcp binding**
- **clear ip dhcp conflict**
- **debug ip dhcp client**
- **debug ip dhcp server**
- **clear ip dhcp server statistics**
- **show dhcp lease**

- **show ip dhcp binding**
- **show ip dhcp conflict**
- **show ip dhcp server statistics**

21.2.1 clear ip dhcp binding

To clear the DHCP binding table, use the **clear ip dhcp binding** command 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 specified IP addresses.

Default No default.

Command mode Privileged mode.

Usage guidelines This command can only clear the DHCP automatic binding, but the DHCP manual 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.

21.2.2 clear ip dhcp conflict

To clear the DHCP conflict record, use the **clear ip dhcp conflict** command 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 specified IP

		addresses.

Default	No default.
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 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 quantity of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns the addresses.
show ip dhcp conflict	Show the address conflict that the DHCP server detects when it assigns the address.

21.2.3 clear ip dhcp server statistics

To reset the counter of the DHCP server, use the **clear ip dhcp server statistics** command in the privileged user mode.

clear ip dhcp server statistics

Default	No default.
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 quantity of various 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.

21.2.4 debug ip dhcp client

To carry out the DHCP Client debugging, use the **debug ip dhcp client** command in the privileged user mode:

debug ip dhcp client

no debug ip dhcp client

Parameter description	None
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 opens the debugging switch of the dhcp client in the equipment. `debug ip dhcp client`
Related commands	

21.2.5 debug ip dhcp server

To carry out the DHCP Server debugging, use the **debug ip dhcp server** command in the privileged user mode:

debug ip dhcp server

no debug ip dhcp server

Parameter description	None.
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 opens the debugging switch of the dhcp server in the equipment. `debug ip dhcp server`
Related commands	

21.2.6 show dhcp lease

To show the lease information obtained by the DHCP client, use the EXEC command **show dhcp lease**.

show dhcp lease

Parameter description	None.
Default	No default behavior.
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 show result of the **show dhcp lease**.

```
DGS-3610# 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
```

21.2.7 show ip dhcp binding

To show the binding condition of the DHCP address, use the EXEC command **show ip dhcp binding**.

show ip dhcp binding [*ip-address*]

Parameter description

Parameter	Description
ip-address	(Optional) Only show the binding condition of specified IP addresses.

Default

No default behavior.

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 output result of the **show ip dhcp binding**.

```
DGS-3610# show ip dhcp binding
IP address      Hardware address   Lease expiration     Type
192.168.12.158 01.00D0.F838.BF3D.  0 days 1 hours 0 mins  Automatic
192.168.12.6    aaaa.aaaa.ab01      Infinite             Manual
```

The meaning of various fields in the output result is described as follows.

Field	Description
IP address	**The IP address to be assigned to the DHCP client.**

Hardware address	**The hardware address of the DHCP client.**
Lease expiration	**The expiration date of the lease.The Infinite indicate it is not limited by the time. The IDLE indicates the address in the free status currently for the possible reason that it is not leased again or the DHCP client releases it actively.**
Type	**The type of the address binding. The Automatic indicates to assign it automatically, and the Manual indicates to assign it manually.**

Related commands	**Command**	**Description**
	clear ip dhcp binding	Clear the DHCP address binding table.

21.2.8 show ip dhcp conflict

To show the conflict history record of the DHCP sever, use the EXEC command **show ip dhcp conflict**.

show ip dhcp conflict

Parameter description	None.
Default	No default behavior.
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.
	`DGS-3610# 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 can not 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.

21.2.9 show ip dhcp server statistics

To show various statistics data of the DHCP server, use the EXEC command **show ip dhcp server statistics**.

show ip dhcp server statistics

Parameter description

None.

Default

No default behavior.

Command mode

Privileged mode.

Usage guidelines

This command can show various statistics data of current DHCP server.

Examples

The following is the output result of the **show ip dhcp server statistics** command.

```
DGS-3610# show ip dhcp server statistics
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	**The quantity of the address pools.**
Automatic bindings	**The quantity of the automatic address bindings.**
Manual bindings	**The quantity of the manual address bindings.**
Expired bindings	**The quantity of the expired address bindings.**
Malformed messages	**The quantity of malformed messages received by the DHCP.**
Message Received or Sent	**The quantity of the messages received and sent by the DHCP server respectively.**

Related commands

Command	Description
clear ip dhcp server statistics	Delete the DHCP service statistic data.

22 Configuring DHCP Relay Command

22.1 DHCP Relay Configuration Command

DHCP configuration includes the following commands:

- **Service dhcp**
- **Ip helper-address**

22.1.1 service dhcp

To enable the DHCP relay agent feature, use the **service dhcp** global configuration mode. The **no** form of this command can disable the DHCP relay agent feature.

service dhcp

no service dhcp

Default	By default, the DHCP relay agent feature is disabled.
Command mode	Global configuration mode.
Usage guidelines	The DHCP agent feature can forward DHCP requests to other servers, and forwards the returned DHCP response packets to the DHCP client, serving as the relay for DHCP packets.
Examples	In the following configuration example, the router has enabled the DHCP server and trunk feature. `service dhcp`

Related commands

Command	Description
ip helper-address [**vrf**] *A.B.C.D*	Add one DHCP server address

22.1.2 ip helper-address

This command allows you to add a DHCP server address. The **no** form of this command deletes a server address.

The server address can be configured globally or for a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information of the appropriate mode.

Default	No server information is configured by default.
Command mode	Global configuration mode and interface configuration mode.
Usage guidelines	In a mode, you can configure multiple dhcp server addresses. One DHCP request of this interface will be sent to multiple servers. You can select one from the multiple responses to confirm. 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	Set the addresses of two servers in the same vrf. One server address is 61.154.26.49, and the address of the vrf-based server with instance name of local is 192.168.197.1.
	`ip helper-address 61.154.26.49`
	`ip helper-address vrf local 192.168.197.1`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay Agent

22.1.3 ip dhcp relay information option dot1x

Use this command configuration to enable the **dhcp option dot1x** function, and use the **no** form of the command to disable the **dhcp option dot1x** function.

Default	Off
Command mode	Global configuration mode.

Usage guidelines	It is necessary to configure to open the DHCP relay, and combines with the 802.1x related configuration, so as to configure this command.
Examples	In the configuration example below, the equipment enables the dhcp option dot1x function. `ip dhcp relay information option dot1x`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay Agent
ip dhcp relay information option dot1x access-group	Configure the option dot1x acl.

22.1.4 ip dhcp relay information option dot1x access-group

Use this command to configure the application **dhcp option dot1x acl**, and use the **no** form of this command to disable the **dhcp option dot1x acl** application.

Default	Don't associate with the ACL.
Command mode	Global configuration mode.
Usage guidelines	It should be noted that no conflict with existing ACE of the configured ACL at the port will appear when this command is configured.
Examples	In the configuration example below, the switch enables the switch. `ip dhcp relay information option dot1x access-group` *`acl-name`*

Related commands

Command	Description
service dhcp	Enable the DHCP Relay Agent
ip dhcp relay information option dot1x	Configure to enable the DHCP option dot1x function.

22.1.5 ip dhcp relay information option82

Use this command to configure to enable the **ip dhcp relay information option82** function, and use The **no** form of this command to disable the **ip dhcp relay information option82** function.

Default	Off

Command mode	Global configuration mode.
Usage guidelines	It is necessary to exclude with the **option dot1x** command when this command is configured.
Examples	In the configuration example below, the switch enables the switch. `ip dhcp relay information option82`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay Agent
ip dhcp relay information option dot1x	Configure to enable the DHCP option dot1x function.

22.1.6 ip dhcp relay check server-id

Use this command to enable the ip dhcp relay check server-id function. Use the **no** form of this command to disable the ip dhcp relay information check server-id function.

Default setting	Disabled.
Command mode	Global configuration mode.
Usage guidelines	When this command is configured, the switch will select the server to send according to the server-id option when it forwards the DHCP REQUES packet.
Examples	In the following example, the device enables the ip dhcp relay check *server-id* function. `ip dhcp relay check server-id`

Related commands

Command	Description
Service dhcp	Enable the DHCP relay agent

22.1.7 ip dhcp relay suppression

This command enables the global DHCP binding. The **no** form of this command disables the global DHCP binding and enables the **DHCP relay** suppression of the port.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	After this command is run, the DHCP request packets of the port are not relayed.

Examples	The following example enables the relay suppression function of port 1.
	`DGS-3610#`
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface fastEthernet 0/1`
	`DGS-3610(config-if)# ip dhcp relay suppression`
	`DGS-3610(config-if)# exit`
	`DGS-3610(config)#`

Related commands	Command	Description
	service dhcp	Enable the DHCP Relay Agent

23 Configuration DNS Module Commands

23.1 Configuring Related Commands

23.1.1 ip domain-lookup

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	Enable the DNS domain name resolution function by default.
Command mode	Global configuration mode.
Usage guidelines	This command is the switch to enable the domain name resolution function. Execute this command to enable the DNS domain name resolution.
Examples	The following example is a switch to enable the DNS domain name resolution function. `DGS-3610(config)# ip domain-lookup`

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

Version description	This command is supported in the version later than v10.1.

23.1.2 ip name-server

This command is to configure the IP address of the domain name server. It will carry out the dynamic domain resolution only when the domain name server is configured. Use the **no** form of this command to delete the configured domain name server.

ip name-server *ip-address*

no ip name-server [*ip-address*]

Parameter description

Parameter	Description
ip-address	The IP address of the domain name server.

Default configuration

No domain name server is configured, by default.

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 domain name can not be obtained from the first Server, the equipment will attempt to send the DNS request to subsequent several Servers, until the response is received correctly.

The system supports up to 6 servers. When the DNS Server is deleted, if you specify the *ip-address* parameter, only specified server is deleted. Otherwise, delete all DNS server addresses.

Examples

```
DGS-3610(config)# ip name-server 192.168.5.134
```

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

Version description

This command is supported in the version later than v10.1.

23.1.3 ip host

This command is used to configure the mapping of the host name and the IP address manually. Use the **no** form of the command to remove the VLAN.

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

```
DGS-3610(config)# ip host switch 192.168.5.243
```

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

Version description

This command is supported in the version later than v10.1.

23.1.4 clear host

To clear the dynamic host name buffer table, execute this command in the privileged user mode.

clear host [*host-name*]

Parameter description

Parameter	Description
host-name	Can delete some specified dynamic host name buffer. "*" denotes to clear all dynamic host name buffern.

Command mode

Privileged mode

Usage guidelines	The mapping record of the host name buffer table comes from 1) by the **ip host** static configuration, 2) by the DNS dynamic learning. Execute this command to delete the host name record learnt by the DNS dynamically.
Examples	The following configuration will delete the mapping record learnt from the host name IP address buffer table dynamically. `clear host *`

Related commands

Command	Description
show hosts	Show the host name buffer table.

Version description	This command is supported in the version later than v10.1.

23.1.5 show hosts

Use this command to display DNS configuration.

show hosts

Command mode	Privileged mode.
Usage guidelines	Show the DNS related configuration information.

Examples

```
DGS-3610# show hosts
Name servers are:
static
host              type         address
switch            static       192.168.5.243
www.dlink.com.tw   dynamic      192.168.5.123
```

Related commands

Command	Description
ip host	Configure the host name and IP address mapping by manual.
ip name-server	Configure the DNS server.

Version description	This command is supported in the version later than v10.1.

24 Configuring NTP Commands

24.1 Configuring NTP Related Commands

DHCP configuration includes the following commands:

- **no ntp**
- **ntp authenticate**
- **ntp authentication-key**
- **ntp disable**
- **ntp server**
- **ntp synchronize**
- **ntp trusted-key**

24.1.1 no ntp

Disable the **ntp** synchronization service to stop the synchronization with the time server and clear all configuration information of **ntp**.

no ntp

Parameter description	None.
Default	The NTP service is disabled by default.
Command mode	Global configuration mode.
Usage guidelines	By default, the NTP function is disabled. However, once the NTP server or NTP security identification mechanism is configured, the NTP function will be enabled.

Examples

The configuration example below disables the NTP service.

```
no ntp
```

Related commands

Command	Description
ntp server	Specify a NTP server.

24.1.2 ntp authenticate

Configure the NTP service to use the NTP global authentication mechanism.

ntp authenticate

no ntp authenticate

Parameter description

None.

Default

The NTP global authentication mechanism is disabled, by default.

Command mode

Global configuration mode.

Usage guidelines

If the global security identification mechanism is not used, the synchronization communication is not encrypted. Enable the global security identification mechanism and configure other global key at the same time, to launch the encryption communication on the server.

The authentication standard is the trust key specified by **ntp authentication-key** and **ntp trusted-key**.

Examples

After corresponding global authentication key is configured and specified as the global trust key, open the authentication mechanism.

```
ntp authentication-key 6 md5 wooooop
ntp trusted-key 6
ntp authenticate
```

Related commands

Command	Description
ntp authentication-key	Set the global authentication key.
ntp trusted-key	Configure the global trust key.

24.1.3 ntp authentication-key

Configure the NTP server with a global NTP authentication key.

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

no ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

Parameter description

Parameter	Description
key-id	The key ID.
key-string	The key string.
enc-type	(Optional) Whether this key is encrypted, where, 0 indicates to not encrypt, 7 indicates to encrypt simply.

Default

No key.

Command mode

Global configuration mode.

Usage guidelines

Configure the global authentication key and adopt the **md5** to encrypt. 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 trust key.

The upper 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.

```
ntp authentication-key 6 md5 wooooop
```

Related commands

Command	Description
ntp authenticate	Enable the global security identification mechanism.
ntp trusted-key	Configure the global trust key.
ntp server	Specify an NTP server.

24.1.4 ntp disable

Disable the NTP message receiving function of corresponding interface.

ntp disable

Parameter description	None.
Default	The interfaces can receive the NTP message by default.
Command mode	Interface configuration mode.
Usage guidelines	The NTP message received from 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 corresponding interface. Note: The interface which can carry out this configuration can configure the IP receiving and sending message. There is no this command in other interface.
Examples	The configuration example below disables the receiving of the NTP message of the interface. `no ntp`
Related commands	

24.1.5 ntp server

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 corresponding server.
prefer	(Optional) Specify corresponding server as the system 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 upper limit of supported synchronous servers are 20. To carry out the encryption communication with the server, set the global encryption key and global trust key firstly, and then specify corresponding key as the trust key of the server to launch the encryption communication of the server. It requires the server present identical global encryption key and global trust key to complete the encryption communication with the server. Prefer to the prefer clock to carry out the synchronization under the same condition. It should be noted that the configured interface is that configured with the IP and can communicate with corresponding NTP server when you configure the source interface of the NTP sending message.
Examples	The configuration example below configures the equipment in the network as NTP server. `ntp server 192.168.210.222`

Related commands

Command	Description
no ntp	Disable the NTP service function.

24.1.6 ntp synchronize

Carry out the NTP real-time synchronization.

ntp synchronize

no ntp synchronize

Parameter description	None.
Default	None.
Command mode	Global configuration mode.

Usage guidelines	The initial synchronization with each server for the NTP is continuous 8 messages, and then it will carry out the synchronization every other 1 minute. During the interval of the automatic synchronization, use this command to carry out the instant synchronization.
Examples	The configuration example below carries out the real time synchronization of NTP. `ntp synchronize`

Related commands

Command	Description
ntp server	Specify one NTP server and carry out the synchronization.

24.1.7 ntp trusted-key

Set the key corresponding to one ID at the global trust key.

ntp trusted-key *key-id*

no ntp trusted-key *key-id*

Parameter description

Parameter	Description
key-id	The global trust key ID.

Default	No trust key by default.
Command mode	Global configuration mode.
Usage guidelines	The NTP communication parties must use the same trust key, and the key is found by ID and is not transmitted, so it improves the security.

Examples	The following example configures an authentication key and sets it as the corresponding server trusted key.
	`ntp authentication-key 6 md5 wooooop`
	`ntp trusted-key 6`
	`ntp server 192.168.210.222 key 6`

	Command	Description
Related commands	**ntp authenticate**	Enable the security authentication mechanism.
	ntp authentication-key	Set the NTP authentication key.
	ntp server	Specify a NTP server.

24.2 Showing and Monitoring Commands

- **debug ntp**
- **show ntp status**

24.2.1 debug ntp

Show the NTP debugging information.

debug ntp

no debug ntp

Parameter description	None.
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. `debug ntp`
Related commands	None.

24.2.2 show ntp status

Show the NTP information.

show ntp status

Parameter description	None.
Default	No default behavior
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. `show ntp status`
Related commands	None.

25 Configuring UDP-Helper Module Commands

25.1 Configuring Related Commands

25.1.1 udp-helper enable

The **udp-helper enable** command is used to enable the forwarding function of the UDP broadcast message. The **no udp-helper enable** command is used to activate the relay 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	None.
Default configuration	By default, the relay forward of the UDP broadcast message is in the disabled status.
Command mode	Global configuration mode.
Usage guidelines	Enable the forwarding function of UDP-Helper, it will forward the UDP broadcast message of the port 69,53,37,137,138,49 by default.
Examples	The following example enables the UDP forwarding function. `DGS-3610(config)# udp-helper enable`

Related commands

Command	Description
ip forward-protocol	Configure the UDP port to be forwarded.

Version description

This command is supported in the version later than v10.1.

25.1.2 ip helper-address

Configure the destination server which the UDP broadcast message will be forwarded to.Use no option to delete the destination server which the UDP broadcast message will be forwarded to.

ip helper-address *address*

no ip helper-address *address*

Parameter description

Parameter	Description
address	Configure the destination server which the UDP broadcast message will be forwarded to in the dotted decimal format, and each interface can support up to 20 server addresses.

Default configuration

No destination server which the UDP broadcast message will be forwarded to is configured.

Command mode

Interface configuration mode.

Usage guidelines

Can configure up to 20 destination servers for each interface. If the destination server of the forwarding is configured at some interface, the broadcast message of specified port received from this interface will be sent to the destination server configured on this interface after the UDP-Helper function is enabled.

Use the **no ip helper-address** to cancel to forward the broadcast message to specified destination server.

Examples

The following example configures the destination server where the UDP broadcast message will be forwarded to.

```
DGS-3610(config-if)# ip helper-address 192.168.100.1
```

Related commands	**Command**	**Description**
	ip forward-protocol	Configure specified UDP ports to be forwarded.

Version description	This command is supported in the version later than v10.1.

25.1.3 ip forward-protocol

This command is to configure specified UDP ports to be forwarded.Use the **no** form of this command to cancel the forward function of specified UDP port broadcast packet.

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	Configure the ports to be forwarded. If this parameter is not specified, it will forward the broadcast message of the 69,53,37,137,138,49 port by default.
	tftp	Trivial File Transfer Protocol(69) Specify this parameter to forward the broadcast message of the UDP port 69.
	domain	Domain Name System(53) Specify this parameter to forward the broadcast message of the UDP port 53.
	time	Time service(37) Specify this parameter to relay forward the broadcast message with the UDP port number 37.
	netbios-ns	NetBIOS Name Service(137) Specify this parameter to forward the broadcast message of the UDP port 137.
	netbios-dgm	NetBIOS Datagram Service(138) Specify this parameter to forward the broadcast message of the UDP port 138.
	tacacs	TAC Access Control System(49) Specify this parameter to forward the broadcast message of the UDP port 49.

Default	No UDP ports to be forwarded is configured.

configuration

Command mode

Global configuration mode.

Usage guidelines

Enable the UDP-Helper function to forward the broadcast message of the UDP port 69,53,37,137,138,49 without any additional configuration by default. Otherwise, it should be configured according to the requirement.

```
DGS-3610(config)# ip forward-protocol udp 134
```

Related commands

Command	Description
udp-helper enable	Enable forwarding of the UDP broadcast message.
ip forward-protocol	Configure specified UDP ports to be forwarded.

Version description

This command is supported in the version later than v10.1.

26 Configuring SNMP Command

26.1 Configuring Related Commands

The SNMP configuration includes the following related commands:

- **no snmp-server**
- **show snmp**
- **snmp-server chassis-id**
- **snmp-server community**
- **snmp-server contact**
- **snmp-server enable traps**
- **snmp-server host**
- **snmp-server location**
- **snmp-server packetsize**
- **snmp-server queue-length**
- **snmp-server system-shutdown**
- **snmp-server trap-source**
- **snmp-server trap-timeout**

26.1.1 no snmp-server

To disable the SNMP agent function, execute the global configuration command **no snmp-server**.

no snmp-server

Default configuration	Disable the SNMP agent function.
Command mode	Global configuration mode.
Usage guidelines	This command disables the SNMP agent services of all versions supported by the router.

Examples

The example below disables the SNMP agent service.

```
DGS-3610(config)# no snmp-server
```

26.1.2 snmp-server chassis-id

To specify the SNMP system sequential number, execute the global configuration command **snmp-server chassis-id**. The **no** form of this command is used to restore 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 sequential number is 60FF60.

Command mode

Global configuration mode.

Usage guidelines

The SNMP system sequential number is generally the sequential number of the machine to facilitate the router identification. The router sequential number can be viewed through the **show snmp** command.

Examples

The example below specifies the SNMP system sequential number 123456:

```
DGS-3610(config)# snmp-server chassis-id 123456
```

Related commands

Command	Description
show snmp	Check the SNMP statistic information

26.1.3 snmp-server community

To specify the SNMP community access string, execute the global configuration command **snmp-server community**. The **no** form of the command cancels the SNMP community access string.

snmp-server community *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [*number*]

no snmp-server community *string*

Parameter description

Parameter	Description
string	Community string, which is equivalent to the communication password between NMS and SNMP.
view-name	Specify the view name for the view-based management.
ro	Specify the MIB variable read-only for the NMS.
rw	Specify the MIB variable read-write for the NMS.
number	Access list sequential number (0-99), associated with the specified access list, specifying the range of NMS addresses that can access the MIB
ipaddr	Associated with the NMS address, specifying the NMS address that can access the MIB.

Default configuration

All community is read-only by default.

Command mode

Global configuration mode.

Usage guidelines

This command is the first important command to enable the SNMP agent function of the router. 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 accesses to the MIB through the access list, which allows only the NMS at address 192.168.12.1 to access the MIB.

```
DGS-3610(config)# access-list 2 permit 192.168.12.1
DGS-3610(config)# access-list 2 deny any
DGS-3610(config)# snmp-server community public ro 2
```

Related commands

Command	Description
access-list	Define the access list

26.1.4 snmp-server contact

To specify the SNMP system contact, execute the global configuration command **snmp-server contact**. 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 contact method of the system

Default configuration

The contact method of the system is empty.

Command mode

Global configuration mode.

Examples

The example below specifies the contact method of the SNMP system as i-net800@i-net.com.cn:

```
DGS-3610(config)# snmp-server contact i-net800@i-net.com.cn
```

Related commands

Command	Description
show snmp-server	Check the SNMP information
no snmp-server	The SNMP agent function is disabled.

26.1.5 snmp-server enable traps

To enable the SNMP to actively send Trap massage to NMS to report the occurring of some emergent and important event, execute the global configuration command **snmp-server enable traps**. The **no** form of this command is used to disable the SNMP to actively send Trap massage to NMS.

snmp-server enable traps [*snmp*]

no snmp-server enable traps

Parameter description

Parameter	Description
snmp	Enable the trap notification for SNMP events

Default configuration

The trap message is disabled by default.

Command mode	Global configuration mode.
Usage guidelines	This command must work with the global configuration command **snmp-server** to be able to send trap messages.

Examples	The example below enables active sending of SNMP event trap messages.
	`DGS-3610(config)# snmp-server enable traps snmp`
	`DGS-3610(config)# snmp-server host 192.168.12.219 public snmp`

Related commands

Command	Description
snmp-server host	Specify the SNMP host

26.1.6 snmp-server host

To specify the SNMP host (NMS) to send the trap message, execute the global configuration command **snmp-server host**. The **no** form of this command is used to cancel the specified SNMP host.

snmp-server host *host-addr* **traps** [**version** {**1 | 2c | 3** [**auth | noauth | priv**]] *community-string* [*notification-type*]

no snmp-server host *host-addr*

Parameter description

Parameter	Description
host-addr	SNMP host address
vrfname	Set the VRF forwarding table
version	Select the snmp version: V1, V2C or V3
auth | *noauth* | *priv*	Set the security level of V3 users.
community-string	Community string or username (V3 version)
Port-num	Set the SNMP host
notification-type	The type of trap sent actively, such as **snmp**.

Default configuration	No default SNMP host is specified by default. If no trap type is specified, all trap types will be included.
Command mode	Global configuration mode.

Usage guidelines

This command must work with the global configuration command **snmp-server enable traps** to actively send trap messages to NMS.

It is possible to configure multiple SNMP hosts to receive the trap messages. One host can use different combinations of the trap types, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different trap messages of to the same host, different trap combinations have to be configured.

Examples

The example below specifies an SNMP host to receive the SNMP event trap:

```
DGS-3610(config)# snmp-server host 192.168.12.219 public snmp
```

Related commands

Command	Description
snmp-server enable traps	Enable sending of trap message

26.1.7 snmp-server location

To set the SNMP system location information, execute the global configuration command **snmp-server location**. The **no** form of this command is used to cancel 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

The system information is empty.

Command mode

Global configuration mode.

Examples

The example below specifies the system information:

```
DGS-3610(config)# snmp-server location start-technology-city 4F of
A Buliding
```

Related

Command	Description

commands	**snmp-sever contact**	System contact information

26.1.8 snmp-server packetsize

To control maximum size of SNMP packet, execute the global configuration command **snmp-sever packetsize**. The **no** form of this command is used to restore default.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter description

Parameter	Description
byte-count	Packet size, 484 bytes ~ 17876 bytes

Default configuration

1,500 bytes by default.

Command mode

Global configuration mode.

Examples

The example below specifies the maximum SNMP packet size as 1,492 bytes:

```
DGS-3610(config)# snmp-server packetsize 1492
```

Related commands

Command	Description
snmp-server queue-length	SNMP queue size

26.1.9 snmp-server queue-length

To specify the length of trap message queue, execute the global configuration command **snmp-server queue-length**.

snmp-server queue-length *length*

Parameter description

Parameter	Description
length	Queue length, 1 ~ 1000

Default configuration

10

Command mode	Global configuration mode.
Usage guidelines	The trap message queue is used to store the trap messages. This command can be used to adjust the size of message queue to control the message send speed. The maximum speed to send messages is 4 messages per second.
Examples	The example below specifies the speed to send trap message is 4 messages per second: `DGS-3610(config)# snmp-server queue-length 4`

Related commands

Command	Description
snmp-server packetsize	Specify the maximum size of SNMP packet

26.1.10 snmp-server system-shutdown

To enable the SNMP system restart notification function, execute the global configuration command **snmp-server system-shutdown**. 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	The SNMP system restart notification function is disabled.
Command mode	Global configuration mode.
Usage guidelines	This command is used to enable the SNMP system restart notification function. DGS-3610 series sends trap messages to the NMS to notify the system pending before the router is reloaded or rebooted.
Examples	The example below enables the SNMP system restart notification function: `DGS-3610(config)# snmp-server system-shutdown`

26.1.11 snmp-server trap-source

To specify the SNMP source address, execute the global configuration command **snmp-server trap-source**. The **no** form of this command is used to restore default.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter description

Parameter	Description
interface	Interface to be used as the SNMP source address

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 SNMP source address:

```
DGS-3610(config)# snmp-server trap-source fastethernet 0
```

Related commands

Command	Description
snmp-server enable traps	Enable active sending of trap message
snmp-server enable host	Specify the NMS host

26.1.12 snmp-server trap-timeout

To define the trap message resend timeout time, execute the global configuration command **snmp-server trap-timeout**. The **no** form of this command is used to restore default.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter description

Parameter	Description
seconds	Timeout period, in seconds

Default configuration

30s

Command mode

Global configuration mode.

Examples

The example below specifies the timeout period as 60 seconds.

```
DGS-3610(config)# snmp-server trap-timeout 60
```

Related commands

Command	Description
snmp-server queue-length	Specify the length of the trap message queue
snmp-server enable host	Specify the NMS host

26.1.13 snmp-server user

To set the SNMP name, execute the global configuration mode command **snmp-server user**. The **no** form of this command is used to delete the user.

snmp-server user *username groupname* {**v1 | v2 | v3** [**encrypted**] [**auth** {**md5 | sha**} *auth-password*] [**priv des56** *priv-password*]} [**access** {*num* | *name*}]

no snmp-server user *username groupname* {**v1 | v2c | v3** }

Parameter description

Parameter	Description
username	User Name
groupname	It is the group name of the user.
v1 | v2 | v3	Specify the SNMP version. But only v3 supports the following security parameters.
encrypted	Specify that the password is displayed in cipher text. If it is not set, the password is displayed in clear text. Input sequential numbers in HEX to create a key if you specify encrypted text. Please 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 authentication is used. **md5** specifies to use the authentication protocol of MD5. **sha** specifies the use of SHA authentication protocol. *auth-password*: It sets the password string (no more than 32 characters) used by the authentication protocol. The system will change the password to authentication key
priv	Specify whether encryption is used. **des56** specifies the use of 56-bit DES encryption protocol. *priv-password* is password string (no more than 32 characters) used for encryption. The system will change the password to encryption key

Default configuration

By default, no user is set.

Command mode

Global configuration mode.

Examples

The example below configures an snmpV3 user with md5 authentication and DES encryption:

```
DGS-3610(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

Related commands

Command	Description
show snmp user	Show the user configuration

26.1.14 snmp-server group

To set the SNMP user group, execute the global configuration mode command **snmp-server group**. The **no** form of this command is used to delete the user group.

snmp-server group *groupname* {**v1 | v2c | v3** {**auth | noauth | priv**}} **[read** *readview***][write** *writeview***] [**access {***num* | ***name***}]**

no snmp-server group *groupname* {**v1 | v2c | v3** }

Parameter description

Parameter	Description
v1,*v2c*,*v3*	Specify the SNMP version
auth	Specify that the user message needs to be authenticated and the data does not need to be

	encrypted, available in SNMPv3
noauth	Specify that the user message does not need to be authenticated or encrypted, available in SNMPv3.
priv	Specify that the user message needs to be authenticated and be encrypted, available in SNMPv3.
readview	Associate with a read-only view.
writeview	Associate with a read-write view.

Default configuration

By default, no user group is set.

Command mode

Global configuration mode.

Examples

The example below sets a user group.

```
DGS-3610(config)# snmp-server group mib2user v3 priv read mib2
```

Related commands

Command	Description
show snmp group	Show the user group configuration

26.1.15 snmp-server view

To set the SNMP view, execute the global configuration mode command **snmp-server view.** The **no** form of this command is used 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	Specify the view-name.
oid-tree	The MIB associated with the view, that is, a MIB sub-tree
include	Indicate that the subset of MIB objects included in the view.
exclude	Indicate that the subset of MIB objects removed from the view.

Default configuration	By default, a default view is set to give access to 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). `DGS-3610(config)# snmp-server view mib2 1.3.6.1 include`

Related commands

Command	Description
show snmp view	Show the view configuration

26.2 Showing Related Command

26.2.1 show snmp

To view the SNMP status information, execute the privileged user command **show snmp**.

show snmp [**mib | user | view | group**]

Command mode	Privileged mode
Usage guidelines	**show snmp**: Show relevant statistical information of the SNMP **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

Examples	The example below shows the SNMP statistical information:
	`DGS-3610# 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 1500)
        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*	SNMP system sequential number

27 Configuring RMON command

27.1 Configuration Related Commands

The RMON configuration commands are as follows:

- **rmon collection stats** *index* [**owner** *owner-string*]
- **rmon collection history** *index* [**owner** *owner-string*] [**buckets** *bucket-number*] [**interval** *seconds*]
- **rmon alarm** *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]
- **rmon event** *number* [**log**] [**trap** *community*] [*description-string*]
- **show rmon statistics**
- **show rmon history**
- **show rmon events**
- **show rmon alarms**

27.1.1 rmon collection stats

This command is used to monitor an Ethernet interface. The **no** form of this command is used to disable the monitoring.

rmon collection stats *index* [**owner** *owner-string*]

no rmon collection stats *index*

Default	No default.
Command mode	Interface configuration mode
Usage guidelines	None.

Examples	The example below enables monitoring the statistics of Ethernet port 1.
	`DGS-3610(config)# interface fast-Ethernet 0/1`
	`DGS-3610(config-if)# rmon collection stats 1 zhansan`

	Command	Description
Related commands	**rmon collection history** *index* [**owner** *owner-name*] **buckets** *bucket-number* **interval** *seconds*	Add a history control entry

27.1.2 rmon collection history

This command is used 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	No default.
Command mode	Interface configuration mode
Usage guidelines	DGS-3610 series allows you to modify the configured history information of the Ethernet network, including the configurations of **owner, buckets**, and **interval**. However, the modification does not take effect immediately. It becomes effective until the recording of the next history information.

Examples	The example below enables monitoring the history of Ethernet port 1.
	`DGS-3610(config)# interface fast-Ethernet 0/1`
	`DGS-3610(config-if)# rmon collection history 1 zhansan buckets 10 interval 10`

	Command	Description
Related commands	**rmon collection stats** *index* [**owner** *owner-name*]	Add a statistical entry

27.1.3 rmon alarm

This command is used 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	No default.
Command mode	Global configuration mode.
Usage guidelines	DGS-3610 series allows you to modify the configured history information of the Ethernet network, including the configurations of **variable, interval, absolute/delta, owner, rising-threadhold/falling-threadhold**, and the corresponding event. However, the modification does not take effect immediately. It becomes effective until the invoking of the next monitoring event.
Examples	The example below monitors the MIB variable instance ifInNUcastPkts.6. `DGS-3610(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 commands

Command	Description
rmon event *number* [**log**] [**trap** *community*] *description string*	Add an event definition.

27.1.4 rmon event

This command is used to define an event. The **no** form of this command cancels the logging.

rmon event *number* [**log**] [**trap** *community*] [*description-string*]

no rmon alarm *number*

Default	No default.

Command mode	Global configuration mode.
Usage guidelines	None.
Examples	The example below defines the event actions: log the event and send a trap message. `DGS-3610(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much " owner zhangsan`

Related commands	**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

27.2 Showing Related Command

27.2.1 show rmon statistics

Show the statistics table information.

show rmon statictics

Default	No default.
Command mode	Privileged mode.
Usage guidelines	None.

Examples	The example below shows the statistics table information.
	`DGS-3610# show rmon statistics`
	`Statistics: 1`
	`Data source: Gi1/1`
	`DropEvents: 0`
	`Octets: 1884085`
	`Pkts: 3096`
	`BroadcastPkts: 161`

```
MulticastPkts: 97
CRCAlignErrors: 0
UndersizePkts: 0
OversizePkts: 1200
Fragments: 0
Jabbers: 0
Conflicts: 0
Pkts64Octets: 128
Pkts65to127Octets: 336
Pkts128to255Octets: 229
Pkts256to511Octets: 3
Pkts512to1023Octets: 0
Pkts1024to1518Octets: 1200
Owner: zhangsan
```

Related commands

Command	Description
rmon collection stats *index* [**owner** *owner-string*]	Add a statistical entry

27.2.2 show rmon history

Show the statistics table information.

show rmon history

Default No default.

Command mode Privileged mode.

Usage guidelines None.

Examples

The example below shows the statistics table information.

```
DGS-3610#  show rmon history
Entry: 1
Data source: Gi1/1
Buckets requested: 65535
Buckets granted: 10
Interval: 1
Owner: zhangsan
Sample: 198
Interval start: 0d:0h:15m:0s
DropEvents: 0
Octets: 67988
```

```
Pkts: 726
BroadcastPkts: 502
MulticastPkts: 189
CRCAlignErrors: 0
UndersizePkts: 0
OversizePkts: 0
Fragments: 0
Jabbers: 0
Conflicts: 0
Utilization: 0
```

	Command	Description
Related commands	**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history control entry

27.2.3 show rmon alarm

Show the statistics table information.

show rmon alarm

Default	No default.
Command mode	Privileged mode.
Usage guidelines	None.
Examples	The example below shows the statistics table information.

```
DGS-3610# show rmon alarm
Event: 1
Description: firstevent
Event type: log-and-trap
Community: public
Last time sent: 0d:0h:0m:0s
Owner: zhangsan
Log: 1
Log time: 0d:0h:37m:47s
Log description: ipttl
Log: 2
Log time: 0d:0h:38m:56s
Log description: ipttl
```

	Command	Description
Related commands	**rmon alarm** *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry

27.2.4 show rmon event

Show the statistics table information.

show rmon event

Default	No default.
Command mode	Privileged mode.
Usage guidelines	None.

Examples	The example below shows the statistics table information.
	`DGS-3610# show rmon event`
	`Alarm: 1`
	`Interval: 1`
	`Variable: 1.3.6.1.2.1.4.2.0`
	`Sample type: absolute`
	`Last value: 64`
	`Startup alarm: 3`
	`Rising threshold: 10`
	`Falling threshold: 22`
	`Rising event: 0`
	`Falling event: 0`
	`Owner: zhangsan`

	Command	Description
Related commands	**rmon event** *number* [**log**] [**trap** *community*] [*description-string*]	Add an event entry

28 Configuring RIP command

28.1 Configuring Related Commands

28.1.1 address-family (RIP)

To access the RIP routing protocol in the address family configuration sub-mode, use this command **address-family**. The **no** form of this command disables 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 RIP address family is not configured.

Command mode

Route configuration mode.

Usage Guidelines

You can use **address-family** to put the router into the address family 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 exit the address family sub-mode and return to the route configuration mode, run **exit-address-family** or **exit**.

Examples

Create a VRF with the name of vpn1 and create its RIP instance for vrf.

```
ip vrf vpn1
exit
interface FastEthernet 1/0
ip vrf forwarding vpn1
ip address 192.168.1.1 255.255.255.0
router rip
!
address-family ipv4 vrf vpn1
network 192.168.1.0
exit-address-family
```

Related commands

Command	Description
exit-address-family	Exit the address family configuration sub-mode
ip vrf	Create a VRF.

Platform description

Version description

28.1.2 auto-summary (RIP)

To enable the RIP route automatic summary function, execute the route protocol configuration command **auto-summary**. The **no** form of this command disables the route automatic summary function.

auto-summary

no auto-summary

Parameter description

No parameter or keyword.

Default configuration

Automatic summary function is enabled by default.

Command mode

Routing process configuration mode.

Usage guidelines

The automatic summary of RIP routes means the subnet routes automatically gather into categorized network routes when passing through categorized network border. Route automatic summary is enabled by default for RIPv1 and RIPv2.

The automatic summary function of the RIP routes improves the flexibility and effectiveness of the network. If the summary route exists, the sub-routes contained in the summary route cannot be seen in the routing table, resulting in great reduction of the routing table scale.

Advertising summary route is more efficient than advertising separate routes because of the following factors:

- Summary 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 it may be hoped to learn the specific sub-routes instead of the summary network route. Here it is required to disable the automatic summary function. Only when the RIPv2 is configured, however, the route automatic summary function can be disabled. For the RIPv1, the route automatic summary is always enabled.

Examples

The configuration example below disables the route automatic summary of the RIPv2.

```
router rip
version 2
no auto-summary
```

Related commands

Command	Description
version	Define the RIP software version: v1 or v2. Both v1 and v2 are supported by default.

Platform description

Version description

28.1.3 default-metric (RIP)

To define the default RIP metric, execute the route configuration command **default-metric**. The **no** form of this command is used to restore default.

default-metric *metric*

no default-metric

Parameter description

Parameter	Description
metric	Default metric value. The valid value range is 1~16. If the metric is greater than or equal to 16, DGS-3610 series regards the route unreachable.

Default configuration

The default value is 1.

Command mode

Routing process configuration mode.

Usage guidelines

This command needs to work with the routing protocol 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 protocol protocols. In 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 overwrite 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 learnt by the OSPF routing protocol, whose initial RIP metric is set as 3.

```
router rip
default-metric 3
redistribute ospf 100
```

Related commands

Command	Description
redistribute	Redistribute the routes from one routing domain to another routing domain.

Platform description	
Version description	

28.1.4 default-information originate(RIP)

This command **default-information originate** generates a default route in the RIP process. The **no** form of this command deletes the generated default route.

default-information originate

no default-information originate

Parameter description	
Default configuration	The default route is not generated.
Command mode	Routing process configuration mode.
Usage guidelines	
Examples	Generate a default route to the RIP routing table. `default-information originat`
Related commands	
Platform description	
Version description	

28.1.5 distance

This command sets the administrative **distance** of the RIP route. The **no** form of this command restores the default setting.

distance *distance* [*ip-address wildcard*]

no distance [*distance ip-address wildcard*]

Parameter description

Parameter	Description
distance	Set the administrative distance of the RIP router. The value is an integer between 1 and 255.
ip-address	Prefix of the source IP address of the route
wildcard	Define the 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

This command sets the administrative distance of the RIP route.

You can use this command to create several administrative distances with source address prefix. When the source address of the RIP route is within the range specified by the prefix, the corresponding administrative distance is applied; otherwise, the route uses the administrative distance set by the RIP.

Examples

Set the administrative distance of the RIP route to **160**, and specify the administrative distance of the route learnt from 192.168.2.1 to **123**.

```
DGS-3610(config)# router rip
DGS-3610(config-router)# distance 160
DGS-3610(config-router)# distance 123 192.168.12.1 0.0.0.0
```

Related commands

Platform description

Version description	

28.1.6 distribute-list in (RIP)

To control the route update for filtering, use the **distribute-list in** routing process configuration command. The **no** form of this command deletes the definition.

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	Specify the ACL. 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) Distribute list, only applied on the specified interface

Default configuration	No distribute list is defined by default.
Command mode	Routing process configuration mode.
Usage guidelines	To deny the reception of some specified routes, you can process all the route update packets received by configuring the route distribute control list. If no interface is specified, the routes received by all interfaces are processed.
Examples	In the following configuration example, the RIP controls and processes the routes received from the Fastethernet 0/0 port, only allowing the reception of the routes starting with 172.16. `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

Parameter	Description
access-list	Define the ACL.
prefix-list	Define the prefix of the ACL.

Platform description

Version description

28.1.7 distribute-list out (RIP)

To control the route update advertisement, use the **distribute-list out** routing process configuration command. The **no** form of this command deletes the definition.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id*]

Parameter description

Parameter	Description
access-list-number	Specify the ACL. Only the routes on the ACL are sent.
prefix *prefix-list-name*	Use the prefix list to filter the routes.
interface	(Optional) Distribute list, where the route update advertisement control is only applied on the specified interface
protocol	(Optional) Distribute list, selectively redistributing the routes of the specified routing process

Default configuration	No LSA control by default.
Command mode	Routing process configuration mode.
Usage guidelines	If the command is run without any optional parameters, the route update advertisement control applies to all port. If with ports, the control applies to only the specified ports. If with other route processes, the specified route processes are filtered for route re-distribution, which is not the control of route update advertisement.

Examples	In the following configuration example, the RIP routing process only advertises the 192.168.12.0/24 route.
	`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

Parameter	Description
access-list	Define the ACL.
prefix-list	Define the prefix of the ACL.
redistribute	Configure route Redistribution

28.1.8 exit-address-family

You can use this command **exit-address-family** to exit the address family configuration mode.

exit-address-family

Parameter description	No parameter or keyword.
Default configuration	This command has no default value.

Command mode

Address family configuration mode.

Usage guidelines

Use this command to exit this configuration mode in the address family configuration mode.

The abbreviation of this command is **exit** .

Examples

The following example shows how to access or exit the mode of address family:

```
DGS-3610(config-router)# address-family ipv4 vrf vpn1
DGS-3610(config-router-af)# exit-address-family
```

Related commands

Parameter	Description
address-family	Enter the address family configuration sub-mode

Platform description

Version description

28.1.9 ip rip authentication key-chain

To enable the RIP authentication and specify the keychain used for RIP authentication, execute the interface configuration command **ip rip authentication key-chain**. 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 that is used to specify the RIP authentication

Default configuration

No RIP packet authentication is specified by default.

Command mode

Interface configuration mode.

Usage guidelines	If the keychain is specified in the interface configuration but not defined with the **key chain** global configuration command, the RIP packet authentication will not occur. The RIPv1 does not support RIP packet authentication but the RIPv2 does.

Examples	The configuration example below enables the RIP authentication n interface serial 0 with the associated keychain is ripchain.
	`interface serial 0/0`
	`ip rip authentication key-chain ripchain`

Related commands

Command	Description
ip rip authentication mode	Define the RIP authentication mode
ip rip receive version	RIP packets of which version are received on an interface
ip rip send version	RIP packets of which version are sent on an interface
key chain	Type in the keychain and enter the keychain configuration mode

Platform description

Version description

28.1.10 ip rip authentication mode

To define the RIP authentication mode, execute the interface configuration command **ip rip authentication mode**. The **no** form of this command is used to restore the default RIP authentication mode.

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

Parameter description

Parameter	Description
text	The RIP authentication mode is plaintext authentication.
md5	The RIP authentication mode is MD5 authentication.

Default configuration	It is the plaintext authentication by default.
Command mode	Interface configuration mode.
Usage guidelines	In configuration RIP authentication, all routers to exchange RIP routing information directly must have the same RIP authentication mode. Otherwise, the RIP packet exchange fails. The RIPv1 does not support RIP packet authentication but the RIPv2 does.

Examples	The configuration example below configures the RIP authentication mode of the interface serial 0 as md5.
	`interface serial 0/0`
	`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 the RIP packet authentication.
key chain	Type in the keychain and enter the keychain configuration mode

Platform description	
Version description	

28.1.11 ip rip receive enable

This command enables a specified port to receive RIP packets. The **no** form of this command prohibits a port from receiving RIP packets.

ip rip receive enable

no ip rip receive enable

Parameter description	This command has no parameters.
Default configuration	The interface is allowed to receive RIP packets by default.
Command mode	Interface configuration mode.
Usage guidelines	To prevent an interface receiving RIP packets, use the **no** form of this command in the interface mode of the port. This command applies to only the port to which this command is configured. The **default** form of this command can restore the prohibition, so that the port can receive the RIP packets again.

Examples	Prohibit the Fastethernet 0/0 from receiving RIP packets.
	`interface fastethernet 0/0`
	`no ip rip receive enable`

Related commands

Parameter	Description
ip rip send enable	Enable or disable a port to send RIP packets
passive-interface	Set RIP passive interface

Platform description	
Version description	

28.1.12 ip rip receive version

To define the RIP packets of which version are received on an interface, execute the interface configuration command **ip rip receive version**. The **no** form of this command is used to restore default.

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.

Usage guidelines

The configuration result of the command overwrites the default configuration of the **version** command. This command affects how the interface receives the RIP messages, which can allow the interface to receive RIPv1 and RIPv2 packets 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 the fastethernet 0/0 interface to receive both RIPv1 and RIPv2 packets.

```
interface fastethernet 0/0
ip rip receive version 1 2
```

Related commands

Command	Description
version	Define the default version of the RIP packets received/sent by all interfaces

Platform description

Version description

28.1.13 ip rip send enable

This command **ip rip send enable** enables RIP to send RIP packets on a specified interface. The **no** form of this command prohibits RIP from sending RIP packets on a specified interface.

ip rip send enable

no ip rip send enable

Parameter description	This command has no parameters.
Default configuration	Sending RIP packets is allowed.
Command mode	Interface configuration mode.
Usage guidelines	To prevent an interface sending RIP packets, use the **no** form of this command in the interface mode of the port. This command applies to only the port to which this command is configured. The **default** form of this command can restore the prohibition, so that the port can send the RIP packets again.

Examples	Prohibit the Fastethernet 0/0 from sending RIP packets.
	`interface fastethernet 0/0`
	`no ip rip send enable`

Related commands

Parameter	Description
ip rip receive enable	Enable or disable a port to receive RIP packets
passive-interface	Set RIP passive interface

Platform description	
Version description	

28.1.14 ip rip send version

To define the RIP packets of which version are sent on an interface, execute the interface configuration command **ip rip send version**. The **no** form of this command is used to restore default.

ip rip send version [**1**] [**2**]

no ip rip send 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

The configuration result of the command overwrites the default configuration of the **version** command. This command affects how the interface sends the RIP messages, which can allow the interface to send RIPv1 and RIPv2 packets 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 the fastethernet 0/0 interface to send both RIPv1 and RIPv2 packets.

```
interface fastethernet 0/0
ip rip send version 1 2
```

Related commands

Command	Description
version	Define the default version of the RIP packets received/send by all interfaces

Platform description

Version description

28.1.15 ip rip v2-broadcast

This command allows the packets of **RIP version 2** to be sent in broadcast rather than multicast mode. The **no** form of this command restores the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter description	This command has no parameters.
Default configuration	The default depends on the configuration of the **version** command.
Command mode	Interface configuration mode.
Usage guidelines	The configuration result of this command can cover the default of the **version** command. This command only affects the behavior of the interface to send RIP packets. You can allow the interface send the packets of both RIPv1 and RIPv2. If no parameters are used in this command, the receiving behavior depends on the **version** setting.

Examples	Set the Fastethernet 0/0 to send RIPv2 packets in the broadcast mode.
	`interface fastethernet 0/0`
	`ip rip v2-broadcast`

Related commands

Parameter	Description
version	Define the default version of the RIP packets received by all interfaces.

Platform description	
Version description	

28.1.16 ip split-horizon (RIP)

To enable the RIP spit-horizon function, execute the interface configuration command **ip split-horizon**. The **no** form of this command disables the RIP split-horizon function.

ip split-horizon

no ip split-horizon

Parameter description

This command has no parameters.

Default configuration

The default activity of horizontal split for all interfaces is enabled.

Command mode

Interface configuration mode.

Usage guidelines

When multiple routers are connected to the IP broadcast network and working with distance vector routing protocol, it is required to use the split-horizon mechanism to prevent the occurring of loop. The split-horizon prevents the router from advertising some routing information from the interface that learns that information, which optimizes the routing information exchange between multiple routers.

For non-broadcast multi-path access network (such as frame relay and X.25), however, the split-horizon may cause some routers cannot 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 an interface enables the split-horizon, execute the **show ip interface** command. The neighbor defined with the **neighbor** command is not affected by the RIP split-horizon.

Examples

The configuration example below disables the RIP split-horizon function on the interface fastethernet 0/0.

```
interface fastethernet 0/0
no ip split-horizon
```

Related commands

Command	Description
neighbor (RIP)	Define RIP neighbor IP address
validate-update-source	Enable RIP route update message source address authentication

Platform description

Version description	If a command or some options exist on some versions, mention that here. If they exist on all platforms, ignore this item.

28.1.17 ip summary-address rip

This command **ip summary-address rip** configures the RIP interface-level convergence of an interface. The **no** form of this command closes the convergence of specified address or subnet.

ip summary-address rip *ip-address ip-network-mask*

no ip summary-address rip *ip-address ip-network-mask*

Parameter description

Parameter	Description
ip-address	IP addresses to be converged
ip-network-mask	Subnet mask of specified IP addresses for route convergence

Default configuration

The RIP is automatically converged to the classful network edge.

Command mode

Interface configuration mode.

Usage guidelines

This command **ip summary-address rip** converges an address or subnet to a specified interface. The RIP is automatically converged to the classful network edge. Only the port convergence can be configured for each classful subnet.

Examples

The following configuration example disables the route summary function of the RIPv2. The port convergence is configured so that the FastEthernet 1/0 advertises the converged route 172.16.0.0/16.

```
interface FastEthernet 1/0
ip summary-address rip 172.16.0.0 255.255.0.0
ip address 172.16.1.1 255.255.255.0
router rip
network 172.16.0.0
version 2
no auto-summary
```

Related commands

Parameter	Description
auto-summary	Enable the automatic summary of RIP route

Platform description

Version description

28.1.18 network (RIP)

To define the list of networks to be advertised in the RIP routing process, execute the routing process configuration command **network**. The **no** form of this command is used to delete the defined network.

network *network-number*

no network *network-number*

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.

Default configuration

Default configuration Routing process configuration mode.

Usage guidelines	When this command is configured, the *network-number* parameter can be the IP address of an interface. DGS-3610 series just consider the number of the natural network. As a result, the entries of 172.16.16.1 and 172.16.0.0 are equivalent. If variable-length mask technology (only supported by the RIPv2) is used in network planning, there are usually multiple interfaces on one router with IP addresses belonging to the same network but not belonging to the same subnet. In this case, the RIPv2 advertises these interfaces to the routes of all subnets. If this is not desired, configure with only the **passive-interface** command. Only when the interface IP address falls into the network list as defined for the RIP, the interface can send RIP route update messages to outside and receive the RIP route update message.
Examples	Example of using the command.
Related commands	Provide the description of the relevant commands. Ignore this item if there is no related command.
Platform description	
Version description	If a command or some options exist on some versions, mention that here. If they exist on all platforms, ignore this item.

28.1.19 neighbor (RIP)

To define the RIP neighbor IP address, execute the routing process configuration command **neighbor**. The **no** form of this command is used to delete the neighbor definition.

neighbor *ip-address*

no neighbor

Parameter description

Parameter	Description
ip-address	IP address of the neighbor. It should be the direct network address of local equipments.

Default configuration

No neighbor is defined by default.

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 it is not desired that the broadcast network or non-broadcast network accesses all routers in the network and all routing information can be received, execute the routing process configuration command **passive-interface** 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.

Examples	The configuration example below defines two network numbers related to RIP.
	`router rip`
	`network 192.168.12.0`
	`network 172.16.0.0`

Related commands	Provide the description of the relevant commands. Ignore this item if there is no related command.
Platform description	
Version description	

28.1.20 offset-list(RIP)

This command increases the metric value of the RIP 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	Number of the standard ACL table
in	Use the ACL to modify the metric of receiving route
out	Use the ACL to modify the metric of sending

	route
offset	Modify the metric value
interface-type	Apply the ACL to the specified port
interface-number	Specify the interface number

Default configuration

The **offset** is not specified.

Command mode

Routing process configuration mode.

Usage guidelines

If a RIP router matches both the **offset-list** of specified port and the global **offset-list** of unspecified port, the RIP route will add the **metric** value of the **offset-list** of specified port.

Examples

Set the metric to grow 7 for the RIP routes in the range specified by ACL 7.

```
offset-list 7 out 7
```

Set the metric to grow 7 for the RIP routes in the range specified by ACL 7 and learnt by fastEthernet 1/0.

```
offset-list 7 in 7
offset-list 8 in 7 fastEthernet 1/0
```

Related commands

Platform description

Version description

28.1.21 output-delay

This command modifies the delay time for the sending of RIP update packets. The **no** form of this command cancels the modification.

output-delay *delay*

no output-delay

Parameter description

Parameter	Description
delay	Set the delay for the packet sending. The value range is from 8 ms to 50 ms.

Default configuration

No sending delay.

Command mode

Routing process configuration mode.

Usage guidelines

Normally, the size of a RIP update packet is 512 Kbytes, and a packet contains 25 routes. If the number of the update routes is larger than 25, the routes are 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 **output-delay** of packet sending on the high-speed device, so that the low-speed device can process all the update packets.

Examples

Set the delay for the sending of RIP update packets to 30 ms.

```
DGS-3610(config)# router rip
DGS-3610(config-router)# output-delay 30
```

Related commands

Platform description

Version description

28.1.22 passive-interface

This command **passive-interface** disables a port to send update packets. The **no** form of this command enables the port to send update packets again.

passive-interface {**default** | *interface-type interface-num*}

no passive-interface {**default** | *interface-type interface-num*}

Parameter description

Parameter	Description
default	Set all ports to the passive mode
interface-type interface-num	Port type and number

Default configuration

No interfaces are set to the 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 some ports to the non-passive mode.

Examples

Set all interfaces to the passive mode and then set ethernet0/0 to the non-passive mode.

```
DGS-3610(config-router)# passive-interface default
DGS-3610(config-router)# no passive-interface ethernet 0/0
```

Related commands

Command	Description
ip rip receive enable	Enable or disable a port to receive RIP packets
ip rip send enable	Enable or disable a port to send RIP packets

Platform description

None

Version description

None

28.1.23 redistribute (RIP)

This command **redistribute** in the route configuration mode sets the external re-distribution route. The **no** form of this command cancels the external re-distribution routes.

redistribute {**bgp** | **isis** |**ospf** | **connected** | **static**}[**metric** *value*] [**route-map** *route-map-name*][**match internal** | **external** *type* | **nssa-external** *type*]

no redistribute {**bgp** | **isis** |**ospf** | **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**	Re-distribution protocol
metric	Set the metric of the re-distribution route
route-map	Re-distribution filtering rule
match	Set the type of OSPF re-distribution route

Default

Command mode

Routing process configuration mode.

Usage guidelines

This command re-distributes the external route into the RIP.

At route redistribution, it is not necessary to convert the metric of one routing protocol into that of another routing protocol, since different routing protocols use distinctively different measurement methods. The RIP metric calculation is based on the hops, while the OSPF metric calculation is based on the bandwidth, so their metrics are not comparable. However, a symbolic metric must be set for route redistribution. Otherwise, route redistribution will fail.

Examples

Re-distribute the static route into the RIP.

```
DGS-3610(config-router)# redistribute static
```

Related commands

Command	Description
default-metric *metric*	Set the default metric of the redistributed route.

Platform description

Version description

28.1.24 router rip

To create the RIP routing process and enter into the routing process configuration mode, execute the global configuration command **router rip**. The **no** form of this command is used to delete the RIP routing process.

router rip

no router rip

Parameter description	No parameter or keyword for the command
Default configuration	No RIP routing process is running.
Command mode	Global configuration mode.
Usage guidelines	One RIP routing process must be defined with one network number. If 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 the routing process configuration mode. `router rip`

Related commands

Command	Description
network (RIP)	Define the network number of the RIP process.

Platform description	
Version description	

28.1.25 timers basic

To adjust the RIP clock, execute the routing process configuration command **timers basic**. The **no** form of this command is used to restore default.

timers basic *update invalid flush*

no timers basic

Parameter description

Parameter	Description
update	Route update time, in seconds. The **update** command defines the period at which the router 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	Invalid period of route, 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 routers 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 30 s, the related routes become invalid and enter into the invalid status. When another 90 s elapses, they will be cleared.
	`router rip`
	`timers basic 10 30 90`
	Note that the small settings of clocks on low-speed links may cause some risks, because the numerous update messages may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or lines above 2Mbps to reduce the time of network route convergence.

Platform description	
Version description	

28.1.26 validate-update-source

To validate the source address of the received RIP route update message, execute the routing process configuration command **validate-update-source**. The **no** form of the command disables the message source address validation.

validate-update-source

no validate-update-source

Version description	No parameter or keyword for the command.
Default configuration	The validation of update message source address is enabled by default.
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 routing process configuration command **validate-update-source**.

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 verification.

```
router rip
no validate-update-source
```

Related commands

Command	Description
ip split-horizon	RIP split-horizon is enabled on the interface.
ip unnumbered	Define the IP unnumbered interface
neighbor (RIP)	Define RIP neighbor IP address

Platform description

Version description

28.1.27 version (RIP)

To define the RIP version number of the whole router, execute the routing process configuration command **version**. The **no** form of this command is used to restore default.

version {**1** | **2**}

no version

Parameter description

Parameter	Description
1	Define the RIP version number as 1.
2	Define the RIP version number as 2.

Default configuration	By default, the route update messages of the RIPv1 and RIPv2 are received only, but those of the RIPv1 is send only.
Command mode	Routing process configuration mode.
Usage guidelines	It is possible redefine the version of RIP to be 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 number as 2.
	`router rip`
	`version 2`

Related commands

Command	Description
ip rip receive version:	Define RIP packets of which version are received on an interface
ip rip send version	Define RIP packets of which version are sent on an interface
show ip rip	Show the information of the currently-running routing protocol process

Platform description	
Version description	

28.2 Showing Related Command

28.2.1 show ip rip

To show the basic information of the RIP routing protocol process, use **show ip rip**.

show ip rip [**vrf** *vrf-name*]

Parameter description

Parameter	Description
vrf *vrf-name*	(Optional) Display the RIP information of specified vrf.

Default configuration

No default configuration.

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 specify the vrf and 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, administrative distance, etc.

```
DGS-3610# 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   Key-chain
    FastEthernet 1/1      2     2     ripkey1
    FastEthernet 1/0      2     2     ripkey2
  Routing for Networks:
    192.168.26.0
    192.168.64.0
  Distance: (default is 50)
```

The following example to specity vrf and display the corresponding basic information of RIP instance:

```
DGS-3610(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)
```

Related commands

Platform description

Version description

28.2.2 show ip rip database

To show the summary address entries in the RIP routing database, run the **show ip rip database** command.

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) Show the subnet number of the routing information.
network-mask	Subnet maskIt must be specified if the network number is specified.

Default configuration

No default configuration.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

Only when the related sub-routes are summarized, the summary address entries appear in the RIP routing database. When the last sub-route information in the summary address entries becomes invalid, the summary address information will be deleted from the database.

Examples

In the configuration example below, all summary address entries in

the RIP routing database are displayed.

```
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 0/0
192.168.121.0/24      auto-summary
192.168.121.0/24      redistributed
[1] via 192.168.2.22, FastEthernet 0/1
```

In the configuration example below, the summary address entries related with 192.168.121.0/24 in the RIP routing database are displayed.

```
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
```

Related commands

Command	Description
show ip rip	Show the information of the currently-running routing protocol process

Platform description

Version description

28.2.3 show ip rip external

To show the external route information of RIP re-distribution, run the **show ip rip external** command.

show ip rip external [**bgp** | **connected** | **isis** | **ospf** | static] [**vrf** *vrf-name*]

Parameter description

Parameter	Description
**bgp	connected	isis	ospf	static**	Show the external route specified by redistribution protocol (optional)
VRF *vrf-name*	Show the RIP external route of specified VRF (optional)

Default configuration

No default configuration.

Command mode	Privileged mode, global configuration mode, routing process configuration mode.
Usage guidelines	

Examples	The following example shows the RIP interface information.
	`DGS-3610# show ip rip interface`
	`FastEthernet 1/1 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 registe: Registed`
	`Interface Summary Rip:`
	`Not Configured`
	`IP interface address:`
	`192.168.64.100/24`

Related commands

Command	Description
show ip rip	Show the information of the currently running routing protocol process.

Platform description	
Version description	

28.2.4 show ip rip interface

To show the RIP interface information, run the **show ip rip interface** command.

show ip rip interface [**vrf** *vrf-name*]

Parameter description

Parameter	Description
VRF *vrf-name*	Show the RIP interface of specified VRF (optional)

Default configuration

No default configuration.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

Examples

The following example shows the RIP interface information.

```
DGS-3610# show ip rip interface
FastEthernet 1/1 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 registe: Registed
    Interface Summary Rip:
      Not Configured
    IP interface address:
      192.168.64.100/24
```

Related commands

Command	Description
show ip rip	Show the information of the currently running routing protocol process.

Platform description

Version description

29 Configuring OSPF command

29.1 Configuration Related Commands

29.1.1 area authentication

To enable the OSPF area authentication, execute the routing process configuration command **area authentication**. The **no** form of the command disables the OSPF area authentication.

area *area-id* **authentication** [*message-digest*]

no area *area-id* **authentication** [*message-digest*]

Parameter description

Parameter	Description
area-id	Specify the area number to enable OSPF authentication. The area number can be a decimal integer or an IP address.
message-digest	(Optional) Use the MD5 (message digest 5) authentication mode

Default configuration

No authentication.

Command mode

Routing process configuration mode.

Usage guidelines

DGS-3610 series supports three authentication types: 1) type 0, no authentication; when no command is executed to enable OSPF authentication, the authentication type in the OSPF packet is type 0; 2) type 1, plaintext authentication mode; when this command is configured, the message-digest option is not used; 3) type 2, MD5 authentication mode; when this command is configured, the message-digest option is used.

All routers in the same OSPF area must have the same

	authentication type. If the authentication is enabled, authentication password must be configured on the interfaces that have connection neighbors. The interface configuration command ip ospf authentication-key can be used to configure the plaintext authentication password. The interface configuration command **ip ospf message-digest-key** 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".
	`DGS-3610(config)#interface FastEthernet 0/0`
	`DGS-3610(config-if)# ip address 192.168.12.1 255.255.255.0`
	`DGS-3610(config-if)# ip ospf message-digest-key 1 md5 backbone`
	`Configure OSPF routing protocol`
	`DGS-3610(config)# router ospf 1`
	`DGS-3610(config-router)# network 192.168.12.0 0.0.0.255 area 0`
	`DGS-3610(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 virtual link

Platform description	
Version description	

29.1.2 area default-cost

To define the cost of the STUB area or NSSA default summary routes (OSPF metric value), execute the route process configuration command **area default-cost**. The **no** form of this command is used to restore default.

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 summary routers to the STUB area or NSSA

Default

The default value is 1.

Command mode

Routing process configuration mode.

Usage guidelines

This command can be configured only on the area border router (ABR) and the ABR must be connected with a STUB area or an NSSA. The so-called ABR router means that the router must be connected to at least one area in addition to the backbone area.

There are three commands to configure an OSPF area as a STUB or NSSA: area stub, area nssa and area default-cost. All routers connected to the STUB must be configured with the **area stub** command, those connected to the NSSA area must be configured with the **area nssa** command, but the **area default-cost** command can be executed only on the ABR.

Examples

The configuration command below sets the cost of the default summary routes to 50.

```
DGS-3610(config)# router ospf
DGS-3610(config-router)# network 172.16.0.0 0.0.255.255area 0
DGS-3610(config-router)#network 192.168.12.0 0.0.0.255area 1
DGS-3610(config-router)# area 1 stub
DGS-3610(config-router)# area 1 default-cost 50
```

Related commands

Command	Description
area stub	Set an OSPF area as the stub area.
area nssa	Set an OSPF area as the NSSA area.

Platform description

Version description

29.1.3 area filter-list

It is set on the ABR to configure the intra-area route filtering conditions between different areas.

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	It is the area ID.
acl-name	Acl name
prefix-name	prefix-list name
access | **prefix**	Associated prefix list or ACL
in | **out**	Configure to apply the condition in routes incoming/outgoing the area

Default

No filtering

Command mode

Routing process configuration mode.

Usage guidelines

This command can be configured only on an Area Board Router (ABR).

It is used when it is necessary to configure the ABR's filtering condition for the route learning between different areas.

Examples

In the configuration command below, it configures the area 1 to learn only the inter-area routes within the range 172.22.0.0/8.

```
DGS-3610# configure terminal
DGS-3610(config)# access-list 1 permit 172.22.0.0/8
DGS-3610(config)# router ospf 100
DGS-3610(config-router)# area 1 filter-list access 1 in
```

Related commands

Platform description	
Version description	

29.1.4 area nssa

To set an OSPF area as an nssa, execute the routing process configuration command **area nssa**. The **no** form of this command is used to delete the NSSA or the configuration of the NSSA.

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	Use this command to import the routing information to common area but not to the nssa area when the switch is an ABR of an nssa area.
default-information originate	(Optional) Generate the default type 7 LSA to the nssa area. This option is valid only on NSSA ABR or ASBR.
no-summary	(Optional) Prevent nssa ABRs from sending types 3 and 4 LSA to 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 different on the nssa ABR and ASBR. On the ABR, the Type-7 LSA default route will be generated on matter whether there are default routes in the routing table; on the ASBR (which is not an ABR at the same time), the Type-7 LSA default route is generated only when the default route exists in the

routing table.

The parameter **no-redistribution** used on the ASBR has the other external routes that OSPF has introduced with the **redistribute** command from advertising to the NSSA area. This optional is generally used when the NSSA router is both an ASBR and an ABR, which prevents external routing information from entering the nssa.

To reduce further the quantity of LSAs sent to the NSSA area, it is possible to configure the no-summary attribute on the ABR, to prevent ABR from advertising summary LSAs (Type-3 LSA) to NSSA area.

In addition, the **area default-cost** is used to connect the ABR of the NSSA area. This command configures the cost for the ABR to send the default route to the NSSA area. By default, the cost of the default route to NSSA is 1.

Examples

The configuration example below sets area 1 as the stub area, which must be executed on routers in that area.

```
DGS-3610(config)#router ospf 1
DGS-3610(config-router)#network 172.16.0.0 0.0.255.255 area 0
DGS-3610(config-router)#network 192.168.12.0 0.0.0.255 area 1
DGS-3610(config-router)# area 1 nssa
```

Related commands

Command	Description
area default-cost	Define the cost (OSPF metric value) of the default summary route advertised to the NSSA.

Platform description

Version description

29.1.5 area range

To configure the route convergence between OSPF areas, execute the route process configuration command **area range**. The **no** form of this command is used to delete the configured route convergence.

area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**]

no area *area-id* **range** *ip-address net-mask*

Parameter description

Parameter	Description
area-id	Specify the OSPF area number with converging route. The area number can be a decimal integer or an IP address.
ip address	Network segment to define converging route
advertise | not-advertise	Whether to advertise the converging range, advertise by default.

Default

No converging route is configured between areas by default.

Command mode

Routing process configuration mode.

Usage guidelines

This command can be executed effectively on the ABR. It is used to converge multiple routes in an area to a single route and advertise this to other areas. The combination of routing information happens only on the border areas. The routers inside the border only see the specific routing information, but only one converging route can be seen outside. The "advertise" and "not-advertise" options can be used to set whether to advertise the converging range, which functions as the filtering and masking purpose. It is advertised by default.

It is possible to define multiple area route convergence commands to simplify the routes in the whole OSPF routing domain, which will improve the network forwarding performance especially in large scale network.

Examples

The configuration example below converge routes in area 1 into a single route 172.16.16.0/20.

```
DGS-3610(config)#router ospf 1
DGS-3610(config-router)#network 172.16.0.0 0.0.15.255 area 0
DGS-3610(config-router)#network 172.16.17.0 0.0.15.255 area 1
DGS-3610(config-router)#area 1 range 172.16.16.0 255.255.240.0
```

Platform description

Version description

29.1.6 area stub

To set an OSPF area as a stub area or full stub area, execute the routing process configuration command **area stub**. 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 ABR needs this parameter.

Default

No stub area is defined by default.

Command mode

Routing process configuration mode.

Usage guidelines

All routers in the OSPF stub area must be configured with the **area stub** command. The ABR only sends three link state advertisement (LSA) to the stub area: 1) type 1, router LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. From the aspect of the routing table, the routers in the stub area can only learn the routes inside the OSPF routing domain, including the internal default routes generated by the ABR. The routers 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 routers in the full stub area can only learn 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 routers 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

The configuration example below sets area 1 as the stub area, which must be executed on routers in that area.

```
DGS-3610(config)# router ospf 1
DGS-3610(config-router)# network 172.16.0.0 0.0.255.255area 0
DGS-3610(config-router)#network 192.168.12.0  0.0.0.255 area 1
DGS-3610(config-router)# area 1 stub
```

Related commands

Command	Description
area default-cost	Define the cost (OSPF metric value) of the default summary route advertised to the STUB area.

Platform description

Version description

29.1.7 area virtual-link

To define the OSPF virtual link, execute the routing process configuration command **area virtual-link**. The **no** form of this command is used to delete the definition of 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. The area number can be 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) 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 text authentication type
message-digest	Set the MD5 authentication type
null	No authentication

Default

dead-interval: 40s
hello-interval: 10s
retransmit-interval: 5s
transmit-delay: 1s
No authentication by default
No default 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 the backbone area is disconnected, it is required to

configure virtual links to connect the backbone domain. 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. Stub Area or NSSA 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 routing process command **area authentication**.

Examples

The configuration example below makes area 1 as the transition area to establish virtual link with neighbor 2.2.2.2.

```
DGS-3610(config)# router ospf 1
DGS-3610(config-router)# network 172.16.0.0 0.0.15.255 area 0
DGS-3610(config-router)# network 172.16.17.0 0.0.15.255 area 1
Switch(config-router)# area 1 virtual-link 192.1.1.1
```

The configuration example below makes 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.

```
DGS-3610(config)# router ospf 1
DGS-3610(config-router)# network 172.16.17.0 0.0.15.255 area 1
DGS-3610(config-router)# network 172.16.252.0 0.0.0.255 area 10
DGS-3610(config-router)# area 0 authentication
message-digest
DGS-3610(config-router)# area 1 virtual-link
1.1.1.1message-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.

Platform description

Version description	

29.1.8 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 Mbps The range is 0-600. 1-2147483647

Default	100Mbps by default
Command mode	Routing process configuration mode.
Usage guidelines	This command sets the reference for automatically generating interface cost. No parameter with it enables the automatic cost function with a default for the reference. A parameter with it enables the automatic cost function with a specified reference. Note that the "default auto-cost" and the "no auto-cost" are different: the former restores the default and enables the automatic cost function while the latter disables the automatic cost 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.
	`DGS-3610(config)# router ospf 1`
	`DGS-3610(config-router)# network 172.16.10.0 0.0.0.255 area 0`
	`DGS-3610(config-router)# auto-cost reference-bandwidth 10`

Related commands

Command	Description
show ip ospf	Show the ospf global configuration information

Platform description

Version description

29.1.9 clear ip ospf process

Clear and restart the OSPF instance.

clear ip ospf (*process-id*) **process**

Parameter description

Parameter	Description
process-id	When this option is used, it clears and restarts the specified OSPF instance. When no process ID is specified, it clears and restarts all 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.

```
DGS-3610#clear ip ospf 1 process
```

Related commands

Platform description

Version description

29.1.10 compatible rfc1583

When the routing table includes several paths to the same destination out of the AS, the first priority route recommended in RFC 1583 or in RFC 2328 will be chosen. Use this command to decide which priority will be taken in RFC 1583 or RFC 2328.

commpatible rfc1583

no commpatible rfc1583

Parameter description	This command has no parameters.
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.
	`DGS-3610(config)# router ospf 1`
	`DGS-3610(config-router)# no commpatible rfc1583`

Related commands

Command	Description
show ip ospf	Show the ospf global configuration information

Platform description

Version description

29.1.11 default-information originate (OSPF)

To generate a default route to the OSPF routing domain, execute the routing process command **default-information originate**. 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) This keyword enables OSPF to 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 types of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric seen 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

No default route is generated by default..

Command mode

Routing process configuration mode.

Usage guidelines

When the **redistribute** or **default-information** command is executed, the OSPF router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate default route automatically or advertise to all 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 ip ospf database** to observe the OSPF link state database. The external links 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 routes.

The route 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 is has a high priority than type 2. As a result, the **show ip route** command shows only the type 1 route.

The routers in the STUB area cannot generate external default routes.

Examples

The configuration example below enables the OSPF to generate an external default route to the OSPF routing domain, with type as 1 and metric as 50.

```
DGS-3610(config)#router ospf 1
DGS-3610(config-router)#network 172.16.24.0 0.0.0.255 area 0
DGS-3610(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

Platform description

Version description

29.1.12 default-metric

To configure the default metric of OSPF redistributed route, execute the routing process command **default-metric**. The **no** form of this command is used to restore default.

default-metric *metric*

no default-metric

Parameter description

Parameter	Description
metric	Define the default 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" routing process configuration 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`
	`DGS-3610(config-router)# network 192.168.12.0`
	`Switch(config-router)# version 2`
	`DGS-3610(config-router)# exit`
	`DGS-3610(config)# router ospf`
	`DGS-3610(config-router)# network 172.16.10.0 0.0.0.255 area 0`
	`Switch(config-router)# default-metric 50`
	`DGS-3610(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

Platform description	
Version description	

29.1.13 distance ospf

Set the administrative distance of the OSPF route of different types.

distance ospf {**intra-area** <*1-255*> | **inter-area** <*1-255*> | **external** <*1-255*>}

no distance ospf

Parameter description

Parameter	Description
intra-area *<1-255>*	Set the inner-area route administrative distance, 110 default.
inter-area *<1-255>*	Set the inter-area route administrative distance, 110 default.
external *<1-255>*	Set the external route administrative distance, 110 default.

Default

The default value is 110.

Command mode

Routing process configuration mode.

Usage guidelines

This command is used to specify different administrative distance for different types of OSPF routes.

Examples

In the configuration below, the OSPF external route administrative distance is set as 160.

```
DGS-3610(config)# router ospf 1
DGS-3610(config-router)# distance ospf external 160
```

Related commands

Platform description

Version description

29.1.14 distribute-list in

Configure LSA filtering.

distribute-list *listname* | **gateway** *plist-name* | **prefix** *plist-name* |

route-map *routemap-name* **in** [**interface-type** *num*]

no distribute-list *listname* | **gateway** *plist-name* | **prefix** *plist-name* |

route-map *routemap-name* **in** [**interface-type** *num*]

Parameter description

Parameter	Description
listname	Use the acl filtering rule.
gateway	Use the gateway filtering rule.
prefix-list	Use the prefix-list filtering rule.
route-map	Use the route-map filtering rule.
interface-type *num*	Configure the LSA route filtering for only a specific interface.

Default

No configuration by default

Command mode

Routing process configuration mode.

Usage guidelines

This configuration filters the received LSA, and only those matching the filtering conditions is involved in the SPF calculation to generate the corresponding routes. It does not affect the link status database or the routing table of the neighbor. 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.

Examples

```
DGS-3610(config)# access-list 3 permit 172.16.0.0 0.0.127.255
DGS-3610(config)# router ospf 25
DGS-3610(config-router)# redistribute rip metric 100
DGS-3610(config-router)# distribute-list 3 in ethernet 1/0
DGS-3610(config-router)# distribute-list 3 in ethernet 1/1
```

Related commands

Platform description

Version description

29.1.15 distribute-list out

Configure filtering re-distribution routes, similar to the **redistribute** command.

distribute-list *listname* | **gateway** *plist-name* | **prefix** *plist-name* |

route-map *map-tag* **out** [**bgp** | **connected** | **isis** | **rip** | **static**]

no distribute-list *listname* | **gateway** *plist-name* | **prefix** *plist-name* |

route-map *map-tag* **out** [**bgp** | **connected** | **isis** | **rip** | **static**]

Parameter description

Parameter	Description
listname	Use the acl filtering rule.
gateway	Use the gateway filtering rule.
prefix-list	Use the prefix-list filtering rule.
route-map	Use the route-map filtering rule.
[**bgp** | **connected** | **isis** | **rip** | **static**]	Source of the routes to be filtered.

Default

No configuration by default

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. But it does not perform route redistribution by itself, working with the **redistribute** command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration. In other words, if the ACL filtering rule is applied on the routes from a source, it is not allowed to configure the prefix-list filter any more.

Examples

The example below filters the redistributed static routes.

```
DGS-3610(config)# router ospf 1
DGS-3610(config)# redistribute static subnets
DGS-3610(config-router)# distribute-list 22 out static
DGS-3610(config-router)# distribute-list prefix jjj out static
% There already has filter configured. Please re-configure.
```

Related commands

Platform description

Version description	

29.1.16 ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of the command to restore the default type.

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Parameter description

Parameter	Description
message-digest	This option indicates MD5 encryption authentication on the interface
null	The option denotes that there is 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** option restores the default of authentication mode. 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 forces 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 0/0.
	`DGS-3610(config)#interface fastethernet 0/0`
	`DGS-3610(config-if)# ip address 172.16.10.0 255.255.255.0`
	`DGS-3610(config-if)# ip ospf authentication message-digest`

Related	Command	Description

commands	**area authentication**	Enable the OSPF area authentication and define the authentication mode
	ip ospf authentication-key	Configure the OSPF plaintext authentication key
	ip ospf message-digest-key	Configure the OSPF MD5 authentication key

Platform description	
Version description	

29.1.17 ip ospf authentication-key

To configure the OSPF plaintext authentication key, execute the interface configuration command **ip ospf authentication-key**. 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, composed of at most 8 letters or numerals.

Default	No authentication key is configured by default.
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 routers that are connected to the same physical network segment must be configured with the same key. To enable the OSPF area authentication, execute the routing process configuration command **area authentication**. The authentication can be enables separately on an interface by

executing the interface mode configuration command **ip ospf authentication**. 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.

```
DGS-3610(config)#interface fastethernet 0/0
DGS-3610(config-if)# ip address 172.16.10.0
255.255.255.0
DGS-3610(config-if)# ip ospf authentication-key ospfauth
```

Related commands

Command	Description
area authentication	Enable the OSPF area authentication and define the authentication mode
Ip ospf authentication	Enable the interface authentication and define the authentication mode

Platform description

Version description

29.1.18 ip ospf cost

To configure the cost (OSPF metric) of the OSPF interface in sending a packet, execute the interface configuration command **ip ospf cost**. The **no** form of this command is used to restore default.

ip ospf cost *cost*

no ip ospf cost

Parameter description

Parameter	Description
cost	OSPF interface cost value.

Default The default cost of the interface is 108/Bandwidth.

Command mode Interface configuration mode.

Usage guidelines

By default, the OSPF interface cost is 10^8/Bandwidth, where Bandwidth is the interface bandwidth, which is configured with the interface configuration command **bandwidth**.

The default OSPF interface costs of several typical lines are as follows:

- 64K serial line: cost is 1562
- E1 line: cost is 48
- 10M Ethernet: cost is 10
- 100M Ethernet: cost is **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 serial 1/0 as 100.

```
DGS-3610(config)# interface serial 1/0
DGS-3610(config-if)# ip ospf cost 100
```

Related commands

Command	Description
bandwidth	Specify the interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Show the ospf global configuration information

Platform description

Version description

29.1.19 ip ospf database-filter all out

This command configures the interface not to advertise LSA messages, that is, the LSA update messages are not sent on the interface. The **no** form of the command restores default.

ip ospf database-filter all out

no ip ospf database-filter

Parameter description

This command has no parameters.

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 prevent an interface from sending LSA update messages, just enable this function on the interface.

Examples	The configuration example below prevents the LSA update messages from being sent on the interface serial 1/0.
	`DGS-3610(config)# interface serial 1/0`
	`DGS-3610(config-if)# ip address 172.16.10.1 255.255.255.0`
	`DGS-3610(config-if)# encapsulation ppp`
	`DGS-3610(config-if)# ip ospf database-filter all out`

Platform description	
Version description	

29.1.20 ip ospf dead-interval

To configure the interval for OSPF to judge the death of interface neighbor, execute the interface configuration command **ip ospf dead-interval**. The **no** form of this command is used to restore default.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameter description

Parameter	Description
seconds	Define the interval to judge the neighbor death, in seconds.

Default	By default it is 4 times of the interval configured with **ip ospf hello-interval**.
Command	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 of 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. Be cautious in using it. There are two points of attentions:

- The death interval cannot be less than the interval of Hello messages.
- The death intervals of all routers on the same network segment must be the same.

Examples

The configuration example below configures the OSPF neighbor death judgment interval on the interface serial 1/0 as 30.

```
DGS-3610(config)# interface serial 1/0
DGS-3610(config-if)# ip address 172.16.10.1
255.255.255.0
DGS-3610(config-if)# encapsulation ppp
DGS-3610(config-if)# ip ospf dead-interval 30
```

Related commands

Command	Description
ip ospf hello-interval	Interval at which the OSPF sends Hello messages

Platform description

Version description

29.1.21 ip ospf disable all

Prohibit a specific interface from generating the OSPF messages.

ip ospf disable all

no ip ospf disable all

Parameter description	This command has no parameters.
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 involve the OSPF calculation.
Examples	DGS-3610(config)# **interface serial** *1/0* DGS-3610(config-if)# **ip address** *172.16.10.1 255.255.255.0* DGS-3610(config-if)# **ip ospf disable all**
Related commands	
Platform description	
Version description	

29.1.22 ip ospf hello-interval

To configure the interval for OSPF to send Hello messages, execute the interface configuration command **ip ospf hello-interval**. The **no** form of this command is used to restore default.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter description

Parameter	Description
seconds	Configure the interval for OSPF to send Hello messages, in seconds.

Default	■ 10 s for Ethernet ■ 10 s for PPP or HDLC encapsulated interfaces ■ 10 s for frame relay PTP interfaces ■ 30 s for non-frame relay PTP sub-interface and X.25 interfaces
Command mode	Interface configuration mode.
Usage guidelines	The interval of 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 of all routers on the same network segment must be the same. To further modify manually the interval to judge neighbor death, it is required to ensure the Hello message interval cannot be greater than the neighbor death interval.

Examples	The configuration example below configures the OSPF Hello message interval on the interface serial 1/0 as 15.
	`DGS-3610(config)# interface serial 1/0`
	`DGS-3610(config-if)# ip address 172.16.10.1 255.255.255.0`
	`DGS-3610(config-if)# encapsulation ppp`
	`DGS-3610(config-if)# ip ospf hello-interval 15`

Related commands

Command	Description
ip ospf dead-interval	Set the OSPF neighbor death judgment interval.

Platform description	
Version description	

29.1.23 ip ospf message-digest-key

To configure the OSPF MD5 authentication key, execute the interface configuration command **ip ospf message-digest-key**. The **no** form of this command is used to delete the MD5 authentication key of OSPF messages.

ip ospf message-digest-key *key-id* **md5** *key*

no ip ospf message-digest-key

Parameter description

Parameter	Description
Key	Key, composed of at most 16 letters or numerals.
key-id	Key identifier, 1~255

Default

No MD5 key is configured by default.

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 routers that are connected to the same physical network segment must be configured with the same key. For neighboring routers, the same key identifier must correspond to the same key.

To enable the OSPF area authentication, execute the routing process configuration command **area authentication**. The authentication can be enabled separately on an interface by executing the interface mode configuration command **ip ospf authentication**. When both the interface and the area are configured with authentication, the one for the interface takes priority.

DGS-3610 series supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an OSPF MD5 authentication key of the router is added, the router will regard other routers 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 routers have been configured with new keys, it is possible to delete the old key.

Examples

The configuration example below add a new OSPF authentication key "hello5" with key ID 5 for the interface FastEthernet 0/0.

```
DGS-3610(config)# interface Serial 1/0
DGS-3610(config-if)# ip address 172.16.24.2
255.255.255.0
DGS-3610(config-if)# encapsulation ppp
DGS-3610(config-if)# ip ospf authentication
```

message-digest

```
DGS-3610(config-if)# ip ospf message-digest-key 10 md5
hello10
DGS-3610(config-if)# ip ospf message-digest-key 5 md5
hello5
```

When all neighbors are added with new keys, the old keys shall be deleted for all routers.

```
DGS-3610(config)# interface Serial1/0
DGS-3610(config-if)# no ip ospf message-digest-key 10 md5 hello10
```

Related commands

Command	Description
area authentication	Enable the OSPF area authentication and define the authentication mode
ip ospf authentication	Enable the interface authentication and define the authentication mode

Platform description

Version description

29.1.24 ip ospf mtu-ignore

To ignore the mtu check when an interface receives the database **description** message, execute the command. The **no** form of this command is used to restore default.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameter description This command has no parameters.

Default The mtu is checked by default.

Command mode Interface configuration mode.

Usage guidelines When the OSPF receives the database description message, it will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an

	interface MTU greater than the received interface 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 serial 1/0.
	`DGS-3610(config)# interface serial 1/0`
	`DGS-3610(config-if)# ip ospf mtu-ignore`

Platform description	
Version description	

29.1.25 ip ospf network

To configure the OSPF network type, execute the interface configuration command **ip ospf network**. The **no** form of this command is used to restore default.

ip ospf network {**broadcast** | **non-broadcast** |

point-to-multipoint [**non-broadcast**] | **point-to-point**}

no ip ospf network {**broadcast** | **non-broadcast** |

point-to-multipoint [**non-broadcast**] | **point-to-point**}

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

By the transmission characteristics of different media, the OSPF divides networks into three types:

- 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 routers can directly communicate, 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 Router shall be elected to advertise the link state of the NBMA network.
- The second is the point-to-multipoint network type. If the topological structure of the network is not a mesh type non-broadcast network, the OSPF requires the interface network type to be configured as the point-to-multipoint network type. In the point-to-multipoint network type, the OSPF regards all inter-router connections as PTP links, involving no election for the designated router. 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 router
- 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 suitable for the full mesh type frame relay connections.

```
DGS-3610(config)# interface Serial1/0
DGS-3610(config-if)# ip address 172.16.24.4
255.255.255.0
DGS-3610(config-if)# encapsulation frame-relay
DGS-3610(config-if)# ip ospf network broadcast
```

The configuration example below configures the frame relay interface network as the point-to-multipoint type, which is suitable for the non-full-mesh type frame relay connections.

```
DGS-3610(config)# interface Serial1/0
DGS-3610(config-if)# ip address 172.16.24.4
255.255.255.0
DGS-3610(config-if)# encapsulation frame-relay
DGS-3610(config-if)# 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 suitable for the full or partial mesh type frame relay connections. The configuration below needs to be done on all branch node routers and non-designated routers (limited to become DR/BDR).

```
DGS-3610(config)# interface Serial1/0
DGS-3610(config-if)# ip address 172.16.24.4
255.255.255.0
DGS-3610(config-if)# encapsulation frame-relay
DGS-3610(config-if)# ip ospf network broadcast
DGS-3610(config-if)# 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, suitable 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

Platform description

Version description

29.1.26 ip ospf priority

To configure the OSPF priority, execute the interface configuration command **ip ospf priority**. The **no** form of this command is used to restore default.

ip ospf priority *priority*

no ip ospf priority

Parameter description

Parameter	Description
Priority	Set the OSPF priority of the interface.

Default

The default priority is 1.

Command mode

Interface configuration mode.

Usage guidelines

The priority of the OSPF interface is included in the Hello message. When DR/BDR (designated router/backup designated router) election occurs in the OSPF broadcast type network, the router with higher priority will become the DR or BDR. If the routers have the same priority, the one with higher ID will become the DR or BDR. The router 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 0/0 as 0.

```
Switch(config)#interface fastethernet 0/0
DGS-3610(config-if)# ip ospf priority 0
```

Related commands

Command	Description
ip ospf network	Configure the OSPF network type of the interface.

Platform description

Version description

29.1.27 ip ospf resync-timeout

Define the maximum period from graceful restart to re-synchronization for the neighbor, "timeout" in case of expiration.

ip ospf resync-timeout *seconds*

no ip ospf resync-timeout

Parameter description

Parameter	Description
Seconds	Set the maximum period limitation for re-synchronization, counting from the receipt of the "restart" signal.

Default

The default is 40 seconds.

Command mode

Interface configuration mode.

Usage guidelines

When an OSPF routing device encounters graceful restart, it notifies the neighbor to re-synchronize the LSDB through the HELLO message. When the neighbor (which must be a GR-aware routing device) receives the message, a synchronization timeout timer is

	initiated. If the routing device does not start the re-synchronization during the period, the neighbor will consider the local routing device as the down status.

Examples	The configuration example below configures the LSU message resend interval on the interface serial 1/0 as 50 seconds.
	`DGS-3610(config)# interface serial 1/0`
	`DGS-3610(config-if)# ip ospf resync-interval 50`

Related commands

Command	Description
ip ospf dead-interval	Set the neighbor death time
ip ospf hello-interval	Set the interval to send the hello message

Platform description	
Version description	

29.1.28 ip ospf retransmit-interval

To define the resend interval of the link state update message of an interface, execute the interface configuration command **ip ospf retransmit-interval**. The **no** form of this command is used to restore default.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter description

Parameter	Description
Seconds	LSU resend interval, in seconds. 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 router 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.

Be cautious in configuring this interval to avoid unnecessary resending. 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 serial 1/0 as 10 seconds.

```
DGS-3610(config)# interface serial 1/0
DGS-3610(config-if)# ip ospf retransmit-interval 10
```

Related commands

Command	Description
area virtual-link	Define OSPF virtual link

Platform description

Version description

29.1.29 ip ospf transmit delay

To define the LSU message transmission delay of the OSPF interface, execute the interface configuration command **ip ospf transmit delay**. The **no** form of this command is used to restore default.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter description

Parameter	Description
Seconds	Define the LSU message transmission delay of the OSPF interface, 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. DGS-3610 series will resend or request resending the LSA with Age up to 3600. If no refresh is obtained in time, the timeout LSA will be cleared from the link state database.

Examples	The configuration example below configures the transmission delay of serial1/ 0 as 5.
	`DGS-3610(config)interface serial 1/0`
	`DGS-3610(config-if)#ip ospf transmit delay 10`

Related commands

Command	Description
area virtual-link	Define OSPF virtual link

Platform description	
Version description	

29.1.30 log-adj-changes

Use this command to configure the log of the neighbor state changes, use the **no** or **default** form of the command to disable it.

log-adj-changes

no log-adj-changes

Parameter description	This command has no parameters.

Default	By default, the function is disabled.
Command mode	Routing process configuration mode.

Examples	The configuration example below turns on the log for neighbor status change.
	`DGS-3610(config)# router ospf 1`
	`DGS-3610(config)# log-adj-changes`

Related commands

Command	Description
show ip ospf	Show the ospf global configuration information

Platform description	
Version description	

29.1.31 max-concurrent-dd

This configuration sets the maximum number of DD messages that can be processed at the same time.

max-concurrent-dd *<1-65535>*

Parameter description

Parameter	Description
<1-65535>	Specify the maximum DD number.

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 each OSPF instance can have how many DD interaction packets maximum at the same time.

Examples

In the configuration example below, the maximum number of DD packets is set as 4.

```
DGS-3610(config)# router ospf 10
DGS-3610(config-router)# max-concurrent-dd 4
```

Related commands

Platform description

Version description

29.1.32 neighbor

To define the OSPF neighbor, execute the routing process configuration command **neighbor**. The **no** form of this command is used 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	Neighbor interface IP address
poll-interval *seconds*	(Optional) Neighbor polling interval, in seconds, 120s 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 network of type "point-to-multipoint [non-broadcast]" supports this option.

Default

No neighbor is defined by default.

Command mode	Routing process configuration mode
Usage guidelines	DGS-3610 series 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 router becomes inactive, in other words, the Hello message is not received within the router 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. Due to no broadcast capability with the point-to-multipoint non-broadcast network, 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 types.

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.
	`DGS-3610(config)# router ospf 20`
	`DGS-3610(config-router)# network 172.16.24.0 0.0.0.255 area 0`
	`DGS-3610(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150`

Related commands

Command	Description
ip ospf priority	Set the priority of the OSPF router.
ip ospf network	Set the OSPF network type

Platform description	
Version description	

29.1.33 network area

To define which interfaces to run OSPF and the OSPF areas they belong to, execute the routing process command **network area**. 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

No OSPF area is 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 through just one command. To run OSPF on an interface, it is required to include the master IP address of the interface in the IP address range as defined with "network area". If the IP address range as defined with "network area" contains only the secondary IP address of the interface, the OSPF will not run on that interface.

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.

```
DGS-3610(config)# router ospf 20
DGS-3610(config-router)# network 172.16.16.0
0.0.15.255 area 172.16.16.0
DGS-3610(config-router)# network 192.168.12.0
0.0.0.255 area 1
DGS-3610(config-router)# network 0.0.0.0 255.255.255.255 area 0
```

Related commands

Command	Description
router ospf	Create OSPF routing process

Platform description

Version description

29.1.34 overflow database

This command is used to configure the maximum number of LSAs supported by the current OSPF instance.

overflow database *<0-4294967294>* **hard** | **soft**

no overflow database

Parameter description

Parameter	Description
<0-4294967294>	Maximum number of LSAs
hard | **soft**	hard: Shut down the OSPF instance when the number of LSAs exceeds that number. soft: Give alarms when the number of LSAs exceeds that number.

Default

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.

```
DGS-3610# config terminal
DGS-3610(config)# router ospf 10
DGS-3610(config-router)# overflow database 10 hard
```

Related commands

Platform description

Version description

29.1.35 overflow database external

This command is used 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 the attempt of restoring normal status.

Default

By default the *max-dbsize* is -1 and the *wait-time* is 0.

Command mode

Global configuration mode.

Usage guidelines

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 the normal status from the overflow status is 3 seconds.

```
DGS-3610# config terminal
DGS-3610(config)# router ospf 10
DGS-3610(config-router)# overflow database external 10 3
```

Related commands

Platform description

Version description

29.1.36 passive-interface

This command is used to configure the specified network interface or all interface of the router as the passive interfaces. The **no** form of this command is used to restore default.

passive-interface [**default** | **type** *number*]

no passive-interface [**default** | **type** *number*]

Parameter description

Parameter	Description
type *number*	Interface that is to be configured as passive interface
default	Set all the interfaces as passive network 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 routers in the network from learning dynamically the routing information of the router, set the specific network interface of this router as passive interface.

Examples

The configuration example below configures the interface serial 1/0 as passive interface.

```
DGS-3610(config)# router ospf 30
DGS-3610(config-router)# passive-interface serial 1/0
```

Related

Command	Description

commands	**show ip ospf interface**	Show the configuration information of the interface

Platform description

Version description

29.1.37 redistribute

This command is used to redistribute the external routing information.

redistribute {**bgp** | **isis** | **rip** | **connected** | **static**}[**metric** *value*

|**metric-type** {*1*|*2*} | **route-map** *map-tag* | **tag** <*0-4294967295*> |

subnets]

no redistribute bgp | **isis** | **rip** | **connected** | **static**

Parameter description

Parameter	Description
bgp | **isis** | **rip** | **connected** | **static**	Redistribute protocol.
metric	Set the metric of the OSPF extern2 LSA.
metric-typ	Set the external routing type as E-1 or E-2
route-map	Redistribution filtering rule
tag	Set the tag value of the routes redistributed to the OSPF.
subnets	Nonstandard networks can be redistributed.

Default

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 broadcast to other OSPF routing device through type-5 LSAs.

Examples

The following command redistributes static routes to the OSPF domain.

```
DGS-3610(config-router)# redistribute static subnets
```

Related commands

Platform description

Version description

29.1.38 router ospf

To create the OSPF routing process, execute the global configuration command **router ospf**. 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	Used to specify the VRF to which the configured OSPF process belongs in the product that supports VRF.

Default

No OSPF routing process by default.

Command mode

Global configuration mode.

Usage guidelines

On the basis of the original implementation, DGS-3610 series firmware v10.1 adds the parameter process ID, extended to multi-instance ospf. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols without mutual interference.

Examples

The configuration example creates the OSPF routing process 10

within the specified vrf: *vpn_1*

```
DGS-3610(config)# router ospf 10 vrf vpn_1
```

Related commands

Command	Description
show ip protocols	Show the brief information of the currently-running routing protocol.
show ip ospf	Show the current ospf process brief information.

Platform description

Version description

29.1.39 router-id

Use this command to set the router ID. Use the **no** form of this command to delete the setting or restore the default router ID.

router-id *router-id*

no router-id

Parameter description

Parameter	Description
router-id	To set the ID of the router, indecates with IP address format.

Default configuration

By default, it will select the maximal interface ip address as the routing device ID by the OSP routing process.

Command mode

Router process configuration mode.

Usage guidelines

Any IP address can be configured as the routing device ID of the routing device. However, the routing device ID of each routing device should be unique. Note that after the change, it will carry out a large number of processing within the protocol, it is not suggested to change the routing device ID, and it will prompt whether it is determined to modify. If you want to change it, it is only allowed only when not any LSA is generated. Hence, when you configure the

OSPF, this configuration should be executed to specify the routing device ID of this routing device. Certainly, you can also specify it by the loopback. At this time, you should configure it before the OSPF is configured.

Examples

The following example modifies the router-id to 0.0.0.36

```
DGS-3610(config)# router ospf 20
DGS-3610(config-router)# router-id 0.0.0.36
```

Related commands

Command	Description
show ip protocols	Shows current routing protocol brief information.

Platform description

Version description

29.1.40 summary-address

To configure the converging route out of the OSPF routing domain, execute the routing process command **summary-address**. The **no** form of this command is used to delete the definition of converging route.

summary-address *ip-address net-mask* **not-advertise | tag** <*0-4294967295*> |]

Parameter description

Parameter	Description
ip address	IP address of the converging route
net-mask	Network mask of the converging route
not-advertise	Do not advertise the convergent route. If not configured, advertise it.

Default

No converging 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 router separately in forms of an external link state. If the incoming routes are a continuous address space, the autonomous border router can advertise only one converging route, which will reduce the scale of routing table greatly.

Unlike the **area rang** command, the "area range" involves the convergence of routes between OSPF areas, while the "summary-address' involves the convergence of external route 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 converging route 100.100.0.0/16.

```
DGS-3610(config)# router ospf 20
DGS-3610(config-router)# summary-address 100.100.0.0 255.255.0.0
DGS-3610(config-router)# redistribute static subnets
DGS-3610(config-router)# network 200.2.2.0 0.0.0.255 area 1
DGS-3610(config-router)# network 172.16.24.0 0.0.0.255 area 0
DGS-3610(config-router)# area 1 nssa
```

Related commands

Command	Description
area-range	Configure route convergence on the OSPF area border router.

Platform description

Version description

29.1.41 timers lsa-group-pacing

This command configures the LSA grouping and then refreshes the whole groups as well as the update interval for aged link state. The **no** form of the command restores default.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing

Parameter description

Parameter	Description
seconds	This parameter is used for time intervals of LSA update, checksum calculation, and aging. The range is 0-1800

Default

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.

```
DGS-3610(config)# router ospf 20
DGS-3610(config-router)# timers lsa-group-pacing 120
```

Related commands

Command	Description
show ip ospf	Show the configuration information of the ospf

Platform description

Version description

29.1.42 timers spf

To configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations, execute the routing process command **timers spf**. The **no** form of this command is used to restore default.

timers spf *spf-delay spf-holdtime*

timers spf *spf-delay spf-holdtime*

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.
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.

Default

spf-delay: 5s; spf-holdtime: 10s.

Command mode

Routing process configuration mode.

Usage guidelines

Smaller values *of spf-delay* and *spf-holdtime* mean OSPF adapts to the topology change faster, which means the network convergence period is shorter, but this will occupy more CPU of the router.

Examples

The configuration example below configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.

```
DGS-3610(config)# router ospf 20
DGS-3610(config-router)# timers spf 3 9
```

Related commands

Command	Description
show ip ospf	Show the configuration information of the ospf

Platform description

Version

description	

29.2 Showing Related Command

29.2.1 show ip ospf

To show the OSPF information summary, execute the privileged user mode command **show ip ospf**.

show ip ospf [*process-id*]

Parameter description	**Parameter**	**Description**
	process-id	OSPF process ID

Default	No default behavior.

Command mode	Privileged mode.

Usage guidelines	This command shows the summary of the operation information of the OSPF routing process.

Examples

The output results of the **show ip ospf** command are as follows:

```
DGS-3610# 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 router 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 router: 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 router-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 supporting TOS0
Supports opaque LSA	Supporting opaque-LSA
Router Type	OSPF router 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 router	Total number of areas on the routers
			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 neighbors in this area	Number of Full neighbors 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.

Platform description	
Version description	

29.2.2 show ip ospf border-routers

To show the OSPF internal routing table to the ABR/ASBR, execute the privileged user mode command **show ip ospf border-routers**.

show ip ospf [*process-id*] **border-routers**

Parameter description

Parameter	Description
process-id	OSPF process ID

Command mode	Privileged 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 "show ip route". The OSPF internal routing table has destination address of the OSPF routing device ID instead of destination network.

Examples

The output results of the **show ip ospf border-routers** command are as follows:

```
DGS-3610# show ip ospf border-routers
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 router.
[2]	Show the cost to the border router.
via 10.0.0.1	Show the next-hop gateway to the border router.
FastEthernet 0/1	Show the interface to the border router.
ABR, ASBR	Show the type of the border router, 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.

Platform description

Version description

29.2.3 show ip ospf database

To show the OSPF link state database information, execute the privileged user mode command **show ip ospf database**.

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-router** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**self-originate** | **max-age**]

show ip ospf [*process-id area-id*] **database** [**router**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**router**] [**adv-router**

ip address

show ip ospf [*process-id area-id*] **database** [**router**] [**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-router** *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-router** *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-router** *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-router** *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-router** *ip-address*]

show ip ospf [*process-id area-id*]**database** [**nssa-external**]

[*link-state-id*] [**self-originate** | **maxage**]

Parameter description

Parameter	Description
area-id	(Optional) Area ID displayed
adv-router	(Optional) Show the LSA information generated by the specified advertising router
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 router itself
maxage	(Optional) Display the LSAs aged
router	(Optional) Show the OSPF router 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 category 10 LSA
opaque-as	(Optional) Show category 11 LSA
opaque-link	(Optional) Show category 9 LSA

Default No default behavior.

Command mode Privileged mode.

Usage guidelines When the OSPF link state database is very large, the itemized displaying is necessary. Proper use of these commands may help OSPF troubleshooting.

Examples

The output results of the **show ip ospf database** command are as follows:

```
DGS-3610# show ip ospf database
OSPF Router with ID (1.1.1.1) (Process ID 1)
            Router Link States (Area 0.0.0.0)
Link ID         ADV Router      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 Router      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 Router      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
             Router Link States (Area 0.0.0.1 [NSSA])
Link ID         ADV Router      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 Router      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 Router      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 Router      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 Router with ID	Display the router id of OSPF link state database and the process number of the corresponding OSPF
Router Link States	Indicate that the following contents are the router LSA information

Net Link States	Indicate that the following contents are the network LSA information
Summary Net Link States	Indicate that the following contents are the summary network LSA information
NSSA-external Link States	Indicate that the following contents are the category 7 autonomous external LSA information
AS External Link States	Indicate that the following contents are the category 5 autonomous external LSA information
Link ID	Link identifier
ADV Router	Identifier of the router that advertises the LSA
Age	Show the live period of the LSA
Seq#	Show the sequential 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 router LSA information
Route	Show the router information included in LSA
Tag	Show the tag of the LSA

The output results of the **show ip ospf database asbr-summary** command are as follows:

```
DGS-3610# show ip ospf database asbr-summary
     OSPF Router 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 Router address)
Advertising Router: 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 Router with ID	Identifier of the router to show the following information and the process number corresponding with OSPF
AS Summary Link States	Indicate that the following contents are the AS summary 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 Router	Show the advertising router of 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
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:

```
DGS-3610# show ip ospf database external
     OSPF Router 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 Router: 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 Router with ID	Identifier of the router to show the following information and the process number corresponding to OSPF
Type-5 AS External Link States	Indicate that the following information is the 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 Router	Show the advertising router of 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	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	Data traffic to the destination network will be forwarded to this IP address. If this address is 0.0.0.0, the data traffic will be forwarded to the router 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:

```
DGS-3610# show ip ospf database network
     OSPF Router 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 Router)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
```

```
Checksum: 0x5366
Length: 32
Network Mask: /24
     Attached Router: 1.1.1.1
     Attached Router: 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 Router with ID	Identifier of the router to show the following information and the process number corresponding to OSPF
Network Link States	Indicate that the following contents are 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 Router	Show the advertising router of 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 network corresponding to the LSA
Attached Router	Show the router that is connected with the network

The output results of the **show ip ospf database router** command are as follows:

```
DGS-3610# show ip ospf database router
     OSPF Router with ID (1.1.1.1) (Process ID 1)
        Router Link States (Area 0.0.0.0)
LS age: 322
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
Link State ID: 1.1.1.1
Advertising Router: 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 router** command are described as follows:

Field	Description
OSPF Router with ID	Identifier of the router to show the following information and the process number corresponding to OSPF
Router Link States	Indicate that the following contents are the router LSA information
LS age	Show the live period of the LSA
Options	Option
Flag	Identifier of router
LS Type	Show the type of the LSA
Link State ID	Show the link ID of the LSA
Advertising Router	Show the advertising router of 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
Number of Links	Show the number of links associated with the router
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:

```
DGS-3610# show ip ospf database summary
     OSPF Router 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 Router: 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 Router with ID	Identifier of the router to show the following information and the process number corresponding to OSPF
Summary Net Link States	Indicate that the following contents are 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 Router	Show the advertising router of 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
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:

```
DGS-3610# show ip ospf database nssa-external
     OSPF Router 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 Router: 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 Router with ID	Identifier of the router to show the following information and the process number corresponding to OSPF
NSSA-external Link States	Indicate the information below is the category 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 Router	Show the advertising router of 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	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
NSSA:Forward Address	Data traffic to the destination network will be forwarded to this IP address. If this address is 0.0.0.0, the data traffic will be forwarded to the router 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:

```
RDGS-3610# show ip ospf database external
     OSPF Router 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 Router: 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 Router with ID	Identifier of the router to show the following information and the process number corresponding to OSPF
Type-7 AS External Link States	Indicate the information below is 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 Router	Show the advertising router of 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	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	Data traffic to the destination network will be forwarded to this IP address. If this address is 0.0.0.0, the data traffic will be forwarded to the router 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:

```
DGS-3610# show ip ospf database database-summary
OSPF process 1:
Router 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	Show the route process ID corresponding to the following information
Router Link	Number of OSPF router LSAs in the area
Network Link	Number of OSPF network LSAs in the area
Summary Link	Number of OSPF net summary LSAs in the area
ASBR-Summary Link	Number of OSPFASBR summary LSAs in the area
AS External Link	Number of OSPF NSSA LSAs in the area
NSSA-external Link	Number of OSPF NSSA LSAs in the router

Platform description

Version description	

29.2.4 show ip ospf interface

To show the OSPF-associated interface information, execute the privileged user mode command **show ip ospf interface**.

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	No default behavior.
Command mode	Privileged mode.
Usage guidelines	This command can show which interfaces are running OSPF as well as the OSPF-related setting information of these interfaces.

Examples

The output results of the **show ip ospf interface FastEthernet** *1/0* command are as follows:

```
DGS-3610# show ip ospf interface fa 1/0

FastEthernet 1/0 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
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 0/0 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	The corresponding MTU
Matching network config	The network area configured for the corresponding OSPF
Process ID	The 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 Router(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated router(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 time 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

Platform description

Version description

29.2.5 show ip ospf neighbor

To show the OSPF neighbor list, execute the privileged user mode command **show ip ospf neighbor**.

show ip ospf [*process-id*] **neighbor** [[**detail**] | [[*interface-type*

interface-number] [*neighbor-id*]]]

Parameter description

Parameter	Description
detail	(Optional) Show the details of neighbor
interface-type interface-number	(Optional) Show the neighbor information of the specified interface
neighbor-id	(Optional) Show the information of the specified neighbor

Default No default behavior.

Command mode Privileged mode.

Usage guidelines This command may display the neighbor information and is usually used to check whether the OSPF is running normally.

Examples The output results of the **show ip ospf neighbor** command are as

follows:

```
DGS-3610# show ip ospf neighbor
OSPF process 1:
Neighbor ID     Pri   State              Dead Time   Address
Interface
3.3.3.3           1   Full/BDR           00:00:32    192.88.88.72
FastEthernet 1/0

DGS-3610# show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 192.88.88.72
    In the area 0.0.0.0 via interface FastEthernet 1/0
    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
```

The fields in the displayed results of the **show ip ospf neighbor** command are described as follows:

Field	Description
Neighbor ID	Neighbor router 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 router
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 router; BDR indicates that the neighbor is the backup designated router; 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 router (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected of the neighbor router (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 router
Neighbor up time	Period from when the router 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

Platform description

Version description

29.2.6 show ip ospf route

Show the OSPF routes.

show ip ospf [*process-id*] **route**

Parameter description

Parameter	Description
process-id	OSPF process ID; show all OSPF routes in case of no parameters.

Default

Command mode

Privileged mode.

Usage guidelines

Examples

```
DGS-3610# 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 1/0
C  192.88.88.0/24 [1] is directly connected, FastEthernet 1/0, 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 corresponding abbreviation and description
100.0.0.0/24	Route prefix
[1]	Route cost
via	Route next hop and interface

Related commands

Platform description

Version description

29.2.7 show ip ospf summary-address

To show the converging router of all OSPF redistribution routes, execute the privileged user mode command **show ip ospf summary-address**.

show ip ospf summary-address

Parameter description This command has no parameters.

Default No default behavior.

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:

```
DGS-3610#show ip ospf summary-address
Summary Address Summary Mask  Advertise  Status  Aggregated subnets
```

```
------------ ------------ ------------ -------- --------------
202.101.0.0    255.255.0.0    advertise    Inactive 0
DGS-3610#
```

Parameter	Description
Summary Address	Converging address
Summary Mask	Converging range
Advertise	Whether to advertise the converging route
Status	The convergence range takes effect or not
Aggregated subnets	How many external routes are included in the range

Platform description

Version description

29.2.8 show ip ospf virtual-link

To show the OSPF virtual link information, execute the privileged user mode command **show ip ospf virtual-link**.

show ip ospf [*process-id*] **virtual-link**

Parameter description This command has no parameters.

Default No default behavior.

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:

```
DGS-3610# show ip ospf virtual-links
```

```
Virtual Link VLINK0 to router 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 router	Show the virtual link neighbor and status
Virtual Link state	State of the virtual link
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 time of the interface
Adjacency State	Neighbor state, where FULL means the stable state

Platform description

Version description

30 Configuring BGP4 Command

30.1 Configuration Related Commands

30.1.1 address-family ipv4

This command is used 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 return to the BGP configuration mode, run the command **exit-address-family.**

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# address-family ipv4
```

Related commands

Command	Description
exit-address-family	Exit the mode.

Platform description

30.1.2 aggregate-address

Use this command to set the aggregate routing entry. You can use the **no** form of the command 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	Prefix of the aggregate address.
mask	Mask of the aggregate address.
as-set	Keep the AS path information of the path in the aggregate address range.
summary-only	Advertise only the summary path

Default configuration

No aggregate configured.

Command mode

BGP configuration mode.

Usage guidelines

By default, the BGP will advertise all path information both before and after aggregation. If you only hope to advertise the aggregated path information, use the **aggregate-address summary-only** command.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# aggregate-address 10.0.0.0
255.0.0.0 as-set
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.

Platform description

30.1.3 auto-summary

This command is used to set the automatic summarization of the BGP route. You can use the **no** form of the command to disable this function.

auto-summary

no auto-summary

Parameter description	This command has no parameters.
Default configuration	By default, no automatic route summarization is performed for the BGP.
Command mode	BGP configuration mode.
Usage guidelines	The automatic route summarization is used to reduce the total volume of the information in the routing table.
Examples	`DGS-3610(config)# router bgp 65000` `DGS-3610(config-router)# auto-summary`

Related commands

Command	Description
router bgp	Enable the BGP protocol.

Platform description

30.1.4 bgp always-compare-med

This command is used to set the BGP 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	This command has no parameters.
Default configuration	By default, it compares the MED of the peer path from the same AS.
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 selection method, this command is not recommended.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# bgp always-compare-med
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath med confed	In electing the best path, allow comparing the MED value of the path of the internal peer from AS.
bgp bestpath med missing-as-worst	In electing the best path, allow setting the priority of the path without MED attribute as the lowest.
bgp deterministic-med	In electing the best path, allow comparing first the path of the peer from the same AS.

Platform description

30.1.5 bgp bestpath as-path ignore

In electing the best path, this command is used 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	This command has no parameters.
Default configuration	By default, the AS path length is considered in choosing the best 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 according to the implement of the standard (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	`DGS-3610(config)# router bgp 65000` `DGS-3610(config-router)# bgp bestpath as-path ignore`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

Platform description

30.1.6 bgp bestpath compare-confed-aspath

In electing the best path, this command allows comparing the ASPATH path lengths of the confederation from the same external routes, smaller ASPATH 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	This command has no parameters.
Default configuration	By default, in electing the best path, it does not compare the ASPATH of the ebgp peer routes inside the same confederation but implements the routing selection by other conditions.
Command mode	BGP configuration mode.
Usage guidelines	By default, in electing the same routing information from the peer of the internal EBGP, the ASPATH of the confederation is not compared. This command is used to compare the ASPATH of the confederation.

	When using this command, note that if a route does not contain the ASPATH of the confederation, it is not possible to implement the ASPATH comparison for that route.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(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 Router ID

Platform description

30.1.7 bgp bestpath compare-routerid

In electing the best path, this command allows comparing the router ID of the same external routes, 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	This command has no parameters.
Default configuration	In electing the best path, 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 path received sequence. You can select the path with smaller Router ID as the optimal path by configuring the following commands.

Examples

```
DGS-3610(config)# router bgp 65000
```

```
DGS-3610(config-router)# bgp bestpath compare-routerid
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp router-id	Set the BGP Router ID

Platform description

30.1.8 bgp bestpath med confed

In electing the best path, this command allows comparing the MED value of the path of the internal peer from AS confederation. 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

By default, it does not compare the MED values of the paths from the peers inside the AS confederation.

Command mode

BGP configuration mode.

Usage guidelines

The MED attribute of the path is transferred between the member ASs inside the confederation. You may set to always compare this value.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# bgp bestpath med confed
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath always-compare-med	In electing the best path, allow comparing the MED value of the path of the peer from different ASs.

	bgp bestpath med missing-as-worst	In electing the best path, allow setting the priority of the path without MED attribute as the lowest.
	bgp deterministic-med	In electing the best path, allow comparing first the path of the peer from the same AS.

Platform description

30.1.9 bgp bestpath med missing-as-worst

In electing the best path, this command sets the priority of the path without MED attribute as the lowest. 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

This command has no parameters.

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 have 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# bgp bestpath med
missing-as-worst
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

	bgp bestpath always-compare-med	In electing the best path, allow comparing the MED value of the path of the peer from different ASs.
	bgp bestpath med confed	In electing the best path, allow comparing the MED value of the path of the internal peer from AS community.
	bgp deterministic-med	In electing the best path, allow comparing first the path of the peer from the same AS.

Platform description

30.1.10 bgp client-to-client reflection

This command turns on the route reflection function between clients on the device. The **no** form of the command turns off the route reflection function between clients.

bgp client-to-client reflection

no bgp client-to-client reflection

Parameter description

This command has no parameters.

Default configuration

This function is turned off on the device.

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 cancelled.

To cancel the client route reflection function, use the command **no bgp client-to-client reflection**.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.11 bgp cluster-id

This command configures the cluster ID of the route reflector. Use the **no** form of the command to restore the default setting.

bgp cluster-id *cluster-id*

no bgp cluster-id [*cluster-id*]

Parameter description

Parameter	Description
cluster-id	Cluster ID of the route reflector, IP address or an integer up to four bytes (must be entered in form of IP address).

Default configuration

router-id of the route reflector

Command mode

BGP configuration mode.

Usage guidelines

In general, one group is only configured with one route reflector. In this case, the Router 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.12 bgp confederation identifier

This command is used to configure the AS confederation identifier. Use the **no** form of the command to restore the default setting.

bgp confederation identifier *as-number*

no bgp confederation identifier

Parameter description

Parameter	Description
as-number	AS confederation identifier. Range: 1 - 65535

Default configuration

No confederation ID.

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

DGS-3610(config-router)# **bgp confederation identifier** 65000

Related

Command	Description

commands	**bgp confederation peers**	Add member AS of the AS confederation.
Platform description		

30.1.13 bgp confederation peers

This command is used 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. The range is from 1 to 65535

Default configuration

No confederation member.

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	`DGS-3610(config-router)# bgp confederation peers 65000 65100`

Related commands

Command	Description
bgp confederation identifier	Configure the confederation identifier.

Platform description

30.1.14 bgp default ipv4-unicast

This command is used to set the "**address family**" as the default IPv4 unicast address. The **no** form of the command turns off the default IPv4 unicast address.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Parameter description

This command has no parameters.

Default configuration

IPv4 address when configuring the BGP session initially

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

```
DGS-3610(config-router)# default ipv4-unicast
```

Related commands

Command	Description
address-family ipv4	Enter the IPv4 address mode.

Platform description

30.1.15 bgp default local-preference

This command is used 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. Range: 0 - 4294967295

Default configuration

The default local priority value is 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

```
DGS-3610(config-router)# bgp default local-preference 200
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath always-compare-med	In electing the best path, allow comparing the MED value of the path of the peer from different ASs.
bgp bestpath med confed	In electing the best 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 best path, allow setting the priority of the path without MED attribute as the lowest.

Platform description

30.1.16 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** form of the command turns off it.

bgp deterministic med

no bgp deterministic med

Parameter description	This command has no parameters.
Default configuration	By default, the function is disabled.
Command mode	BGP configuration mode.
Usage guidelines	By default, they will be compared with each other by 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	`DGS-3610(config-router)# bgp deterministic med`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath always-compare-med	In electing the best path, allow comparing the MED value of the path of the peer from different ASs.
bgp bestpath med confed	In electing the best 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 best path, allow setting the priority of the path without MED attribute as the lowest.

Platform description

30.1.17 bgp enforce-first-as

This command configures rejecting the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number. The **no** form of the command turns off it.

bgp enforce-first-as

no bgp enforce-first-as

Parameter description	This command has no parameters.
Default configuration	No defaulted value.
Command mode	BGP configuration mode.
Usage guidelines	By default, in updating the UPDATE message, the AS number of itself is put into the path section.
Examples	`DGS-3610(config-router)# bgp enforce-first-as`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

Platform description

30.1.18 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 turn off 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	This command has no parameters.
Default	The function is disabled.

configuration	
Command mode	BGP configuration mode.
Usage guidelines	This command takes effect only for the directly-connected EBGP neighbor.
Examples	`DGS-3610(config-router)# bgp faster-external-fallover`

Related commands

Command	Description
router bgp	Enable the BGP protocol

Platform description

30.1.19 bgp log-neighbor-changes

This command enables logging 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	This command has no parameters.
Default configuration	The function is disabled.
Command mode	BGP configuration mode.
Usage guidelines	The **debug** command can also be used to log the BGP status changes. But the "debug" of the BGP may consume a great deal of resources.
Examples	`DGS-3610(config-router)# bgp log-neighbor-changes`

Related commands

Command	Description
router bgp	Enable the BGP protocol

Platform description

30.1.20 bgp router-id

This command is used to configure the ID-IP address of the device used in running the BGP protocol. The **no** form of the command restores the default IP address.

bgp router-id *ip-address*

no bgp router-id *ip-address*

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 route-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

```
DGS-3610(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	Turn on the route dampening function and set the dampening parameters.

Platform description

30.1.21 clear bgp ipv4 unicast

This command is used to reset the BGP.

clear bgp ipv4 unicast {* |*address* **|** *as number* } [[**soft]** [**in** | **out**]]

Parameter description

Parameter	Description
*****	Reset the current all BGP sessions.
address	Reset the BGP session with 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 distributed routing information.
soft	Soft resetting; perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Soft resetting; perform soft resetting for the received routing information.
soft out	Soft resetting; perform soft resetting for the distributed routing information.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

Note: This command is used to require all connected BGP routers to support the route refreshing function. This product supports the route refreshing performance.

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 a new BGP connection.

This product supports to implement a 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 refreshing 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 refreshing performance by the **show ip bgp neighbors** command. If it is supported, you need to execute the **neighbor soft-reconfiguration inbound** command when the input route strategy changes.

Examples

```
DGS-3610# 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.

Platform description

30.1.22 clear bgp ipv4 unicast dampening

This command is used 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

No default configuration.

Command mode

Privileged 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

```
DGS-3610# clear bgp ipv4 unicast 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	Turn on the route dampening function and set the dampening parameters.

Platform description	

30.1.23 clear bgp ipv4 unicast external

This command resets all EBGP connections.

clear bgp ipv4 unicast external [[**soft**] [**in | out**]]

Parameter description	**Parameter**	**Description**
	in	No parameter "soft", reset the session of the peer to establish active connection.
	out	No parameter "soft", reset the session of the local BGP speaker to establish active connection.
	soft	Soft resetting; perform soft resetting for all routing information received/sent from/to the specified peer
	soft in	Soft resetting; perform soft resetting for the received routing information.
	soft out	Soft resetting; perform soft resetting for the distributed routing information.

Default configuration	No default configuration.
Command mode	Privileged mode.
Usage guidelines	This command is used to reset the specified external BGP connection.
Examples	`DGS-3610# clear bgp ipv4 unicast external in`

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp neighbors	Show the neighbor information.

Platform description

30.1.24 clear bgp ipv4 unicast flap-statistics

This command is used to clear the route dampening statistics.

clear bgp ipv4 unicast flap-statistics [*address*[*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration

No default configuration.

Command mode

Privileged 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

```
DGS-3610# clear bgp ipv4 unicast flap-statistics
```

Related commands

Command	Description
bgp dampening	Turn on the route dampening function and set the dampening parameters.
show ip bgp	Show the BGP route entry.

Platform description

30.1.25 clear bgp ipv4 unicast peer-group

This command resets 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	No parameter "soft", reset the session of the peer to establish active connection.
out	No parameter "soft", reset the session of the local BGP speaker to establish active connection.
soft	Soft resetting; perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Soft resetting; perform soft resetting for the received routing information.
soft out	Soft resetting; perform soft resetting for the distributed routing information.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command resets the BGP session with all members in the peer group.

Examples

```
DGS-3610# clear bgp ipv4 unicast peer-group my-group in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

Platform description

30.1.26 clear ip bgp

This command is used to reset the BGP.

clear ip bgp {* |*address* | **ipv4 unicast |** *as number* } [**soft** [**in** | **out**]]

Parameter description

Parameter	Description
*****	Reset the current all BGP sessions.
address	Reset the BGP session with 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 distributed routing information.
soft	Soft resetting; perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Soft resetting; perform soft resetting for the received routing information.
soft out	Soft resetting; perform soft resetting for the distributed routing information.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

Note: This command is used to require all connected BGP routers to support the route refreshing function. This product supports the route refreshing performance.

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 a new BGP connection.

This product supports to implement a 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 refreshing 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 refreshing performance by the **show ip bgp neighbors** command. If it is supported, you need to execute the **neighbor soft-reconfiguration inbound** command when the input route strategy changes.

Examples

```
DGS-3610# clear ip bgp *
```

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.

Platform description

30.1.27 clear ip bgp dampening

This command is used 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

No default configuration.

Command mode

Privileged 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

```
DGS-3610# 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	Turn on the route dampening function and set the dampening parameters.

Platform description

30.1.28 clear ip bgp external

This command resets all EBGP connections.

clear ip bgp external [**ipv4 unicast**] [[**soft**] [**in | out**]]

Parameter description

Parameter	Description
ipv4 unicast	ipv4 unicast session
in	No parameter "soft", reset the session of the peer to establish active connection.
out	No parameter "soft", reset the session of the local BGP speaker to establish active connection.
soft in	Soft resetting; perform soft resetting for the received routing information.
soft out	Soft resetting; perform soft resetting for the distributed routing information.

Default configuration No default configuration.

Command mode Privileged mode.

Usage guidelines This command is used to reset the specified external BGP connection.

Examples

```
DGS-3610# clear ip bgp external in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp neighbors	Show the neighbor information.

Platform description

30.1.29 clear ip bgp flap-statistics

This command is used to clear the route dampening statistics.

clear ip bgp flap-statistics [*address*[*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration

No default configuration.

Command mode

Privileged 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

```
DGS-3610# clear ip bgp flap-statistics
```

Related commands

Command	Description
bgp dampening	Turn on the route dampening function and set the dampening parameters.
show ip bgp	Show the BGP route entry.

Platform description

30.1.30 clear ip bgp peer-group

This command resets 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	No parameter "**soft**", reset the session of the peer to establish active connection.
out	No parameter "**soft**", reset the session of the local BGP speaker to establish active connection.
soft	Soft resetting; perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Soft resetting; perform soft resetting for the received routing information.
soft out	Soft resetting; perform soft resetting for the distributed routing information.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command resets the BGP session with all members in the peer group.

Examples

```
DGS-3610# 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.

Platform description

30.1.31 distance bgp

This command is used to set different administrative distances for different types of BGP routes. The **no** command is used to restore default.

distance bgp *external-distance internal-distance local-distance*

no distance bgp [*external-distance internal-distance local-distance*]

Parameter description

Parameter	Description
external-distance	Administrative distance of the route learnt from the EBGP peers Range: 1 to 255
internal-distance	Administrative distance of the route learnt from the IBGP peers Range: 1 to 255
local-distance	Administrative distance of route learnt from the Peers, but it is considered that the optimal one can be learnt 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 administrative distance of the BGP route. If it is definitely necessary, observe the following points:

1. "*external-distance*" shall have a lower administrative distance than the other IGP routing protocols (OSPF, RIP, etc.);
2. *internal-distance* and *local-distance* shall have higher administrative distance than the other IGP routing protocols.

Examples

```
DGS-3610(config-router)# distance bgp 20 20 200
```

Related

Command	Description

commands	**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.

Platform description

30.1.32 exit-address-family

This command is used to exit the BGP **address-family** configuration mode.

exit-address-family

Parameter description This command has no parameters.

Default configuration None

Command mode BGP **address-family** configuration mode.

Usage guidelines This command can be used to return from various address-family modes of the BGP to the BGP configuration mode.

Examples

```
DGS-3610(config-router-af)#exit-address-family
```

Related commands

Command	Description
address-family ipv4	Enter the **address-family ipv4** configuration mode.

Platform description

30.1.33 ip as-path access-list

This command is used 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 AS path list identifier, range: 1 - 500
permit	Permit the accesses
deny	Deny the accesses
regular-expression	Regular expression Range: 1 to 255 characters.

Default configuration

No list defined.

Command mode

Configuration mode.

Usage guidelines

For the regular expression, see Configuring IP Unicast Route in the configuration guide.

Examples

```
DGS-3610(config-router)# ip as-path access-list hsd 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

Platform description

30.1.34 ip community-list

This command is used to define the community list and control the accesses to it. The **no** form of the command deletes it.

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 No more than 32 characters
standard	Standard community list, number 1-99
expanded	Extended community list, number above 100
permit	Permit the accesses
deny	Deny the accesses
community-number	Community number, in the form of AA:NN (autonomous system number/2-byte numeral), or any of the following predefined values: Internet: Indicate the Internet community, and all paths are of this community. no-export: Indicate this path will not be issued to the \BGP peers. no-export: Indicate this path will not be issued to the BGP peers. local-as: Indicate this path will not be issued to out of this AS. When the confederation is configured, this path will not be issued to other autonomous systems or sub autonomous systems. Range: 1..255 characters.

Default configuration

The community list is not be defined.

Command mode

Global configuration mode.

Usage guidelines

This command is used to define the community list for the BGP.

Examples

```
DGS-3610(config)# ip community-list standard 1 deny 100:20 200:20
DGS-3610(config)# ip community-list standard 1 permit internet
```

Related

Command	Description

commands	**match community-list**	Match community list
	set community-list delete	According to the community list, delete the community attributes in the BGP path attribute
	show ip community-list	Show the information of the community list
	show ip bgp community-list	Show the BGP route information which matches with specified community list.

Platform description	

30.1.35 neighbor activate

This command is used to activate the neighbor or peer group in the current address mode. Use the **no** form of the command to restore the default setting.

neighbor {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

no neighbor {*ip-address* | *peer-group-name*} **advertisement-interval**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
seconds	Time interval to send route update. Range: 1 - 600 seconds

Default configuration	IBGP connection: 15 seconds EBGP connection: 30 seconds
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	DGS-3610(config)# **router bgp** 60 DGS-3610(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.

Platform description

30.1.36 neighbor advertisement-interval

This command sets the time interval to send the BGP route update. Use the **no** form of the command to restore the default setting.

neighbor {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

no neighbor {*ip-address* | *peer-group-name*} **advertisement-interval**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
seconds	Time interval to send route update. Range: 1 - 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

```
DGS-3610(config)# router bgp 60
DGS-3610(config-router)# neighbor 10.0.0.1
advertisement-interval 10
```

Related commands

Command	Description
router bgp	Enable BGP protocol

	neighbor remote-as	Configure the BGP peer.

Platform description

30.1.37 neighbor default-originate

This command allows BGP speaker to advertise 0.0.0.0 as the default route to the peer (group). The **no** form of the command cancels sending the advertisement.

neighbor {*ip-address* | *peer-group-name*} **default-originate**

[**route-map** *map-tag*]

no neighbor {*ip-address* | *peer-group-name*} **default-originate**

[**route-map** *map-tag*]

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
map-tag	Name of the route-map. The name of route map is no more than 32 characters.

Default configuration

Do not send 0.0.0.0 as the default route.

Command mode

BGP configuration mode.

Usage guidelines

This command does not require the default route 0.0.0.0 exist 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

```
DGS-3610(config)# router bgp 60
DGS-3610(config-router)# neighbor 10.1.1.1 remote-as 80
DGS-3610(config-router)# neighbor 10.1.1.1
```

	default-originate

Related commands

Command	Description
router bgp	Enable the BGP protocol
neighbor remote-as	Configure the BGP peer.

Platform description

30.1.38 neighbor description

This command sets a descriptive sentence for the specified peer (group). The **no** form of the command cancels the setting.

neighbor {*ip-address* | *peer-group-name*} **description** *text*

no neighbor {*ip*-address | *peer-group-name*} **description**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
text	Text for describing the peer (group). Range: 80 characters at most

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

```
DGS-3610(config)# router bgp 60
DGS-3610(config-router)# neighbor 10.1.1.1 remote-as 80
DGS-3610(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.

Platform description

30.1.39 neighbor distribute-list

When receiving/transmitting routing information from/to BGP peer, the routing policy is implemented on the basis of ACL. The **no** form of the command cancels the ACL configured.

neighbor {*ip-address* | *peer-group-name*} **distribute-list**

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

no neighbor {*ip-address* | *peer-group-name*} **distribute-list**

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

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
access-list-number	ACL number
in	The ACL applies to the incoming routing information.
out	The ACL applies to the outgoing routing information.

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

For the "**in**" rule or "**out**" rule, this command cannot exist at the same time with the "**neighbor prefix-list**" at any time. 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.

Examples

```
DGS-3610(config)# router bgp 60
DGS-3610(config-router)# neighbor 10.1.1.1 remote-as 80
DGS-3610(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 standard IP ACL or extended IP ACL

Platform description

30.1.40 neighbor ebgp-multihop

This command allows the BGP connection established between the EBGP peers that are not directly connected. The **no** form of the command cancels the setting.

neighbor {ip-address | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*ip-address* | peer-*group-name*} **ebgp-multihop**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
ttl	Maximum hops allowed. 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.

Usage guidelines	To prevent routing loop and dampening, non-default routes that can reach the opposite 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor 10.0.0.1 remote-as 65100
DGS-3610(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.

Platform description

30.1.41 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 {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}

no neighbor {*ip-address* | peer-*group-name*} **filter-list**

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

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
access-list-numbe	as-path list identifying number
in	as-path list applies to the incoming routing information.
out	as-path list applies to the outgoing routing information.

Default configuration	Disabled.
Command mode	BGP 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.

Examples

```
DGS-3610(config)# ip as-path access-list 1 deny _123_
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor 10.0.0.1 remote-as 65100
DGS-3610(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 AS_PATH list
match as-path	Match AS_PATH list

Platform description

30.1.42 neighbor maximum-prefix

This command limits the number of prefixes received from the specified BGP peer. The **no** form of the command cancels the limitation configured.

neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

no neighbor {*ip*-address | *peer-group-name*} **maximum-prefix**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters

	maximum	Upper limit of the number of the received routing information entries
	threshold	Percentage of the maximum when the alarm starts to be generated.
	warning-only	Do not determine the BGP connection when the routing information reaches the upper limit but produce a log entry.

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

By default, the BGP connection will be closed when the received routing information exceeds the upper limit of the setting. If you do not hope to close 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.43 neighbor next-hop-self

When specifying the BGP peer distribution routes, this command is used to set the next-hop of the route to the local BGP speaker. Use the **no** form of the command to disable the configuration.

neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

no neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command is mostly used in the network of not fully mesh type, such as the Frame Relay and X.25, where the BGP speakers within the same subnet cannot completely be accesses mutually.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.44 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 cancels the MD5 authentication.

neighbor {*ip-address* | *peer-group-name*} **password** *string*

no neighbor {*ip-address* | *peer-group-name*} **password**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
string	Use the password of the TCP MD5 authentication. Range:80 characters at most

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command will call the MD5 authentication of the TCP. The BGP peers to connect the BGP connection 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.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor 10.0.0.1 password
D-Link
```

Related commands

Command	Description
router bgp	Enable the BGP protocol
neighbor remote-as	Configure the BGP peer.

Platform description

30.1.45 neighbor peer-group (assigning members)

Use this command to Configure the specified peer to 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 *ip-address* **peer-group** *peer-group-name*

no neighbor *ip-address* **peer-group** *peer-group-name*

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 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**.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor D-Link peer-group
DGS-3610(config-router)# neighbor 10.0.0.1 peer-group D-Link
```

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.

Platform description

30.1.46 neighbor peer-group (creating)

This command creates 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	Specify the name of the peer group. The name of the peer group is within 32 characters

Default configuration

No BGP peer group is created.

Command mode

BGP configuration mode.

Usage guidelines

If multiple BGP peers can 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor D-Link 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 to the member of the BGP peer group.
	show ip bgp peer-group	Show the information of the BGP peer.

Platform description

30.1.47 neighbor prefix-list

When receiving/transmitting routing information from/to BGP peer, this command is used to implement the routing policy on the basis of the prefix list. The **no** form of the command cancels the prefix-list configured.

neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name*} **prefix-list** {**in** |**out**}

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
prefix-lis-name	Nameof the prefix-list It can be up to 32 characters.

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

For the "**in**" rule or "**out**" rule, this command cannot exist at the same time with the "**neighbor distribute-list**" at any time. 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.

Examples

```
DGS-3610(config)# ip prefix-list bgp-filter deny
```

	10.0.0.1/16 DGS-3610(config)# **router bgp** *65000* DGS-3610(config-router)# **neighbor** *10.0.0.1* **prefix-list bgp-filter in**

Related commands

Command	Description
router bgp	Enable the BGP protocol
neighbor remote-as	Configure the BGP peer.
ip prefix-list	Create prefix lists.

Platform description

30.1.48 neighbor remote-as

This command configures the BGP peer (group). The **no** form of the command deletes the configured peer (group).

neighbor {*ip-address* | *peer-group-name*} **remote-as** *as-number*

no neighbor {*ip-address* | *peer-group-name*} **remote-as** *as-number*

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
as-number	BGP peer (group) autonomous system number. Range: 1 to 65535

Default configuration

No BGP peer configured.

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

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor 10.0.0.1 remote-as 80
```

Related commands

Command	Description
router bgp	Enable the BGP protocol

Platform description

30.1.49 neighbor remove-private-as

This command deletes 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 disable the configuration.

neighbor {*ip-address* | *peer-group-name*} **remove-private-as**

no neighbor {*ip-address* | *peer-group-name*} **remove-private-as**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters

Default configuration

The function is disabled.

Command mode

BGP 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.50 neighbor route-map

This command enables route match for the received/sent routes. You can use the **no** form of the command to disable this function.

neighbor {*ip-address*|*peer-group-name* } **route-map** *map-tag* {**in** | **out**}

no neighbor {*ip-address*|*peer-group*-name } **route-map** *map-tag* {**in | out**}

Parameter description

Parameter	Description
ip address	Specify the address for a neighbor
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
map-tag	Name of the match rule
in	The rule applies to the incoming route
out	The rule applies to the outgoing route

Default configuration

No default configuration.

Command mode

BGP configuration mode.

Usage guidelines

This command can be used to filter the incoming and outgoing route for different neighbors by using different incoming/outgoing rules. This can achieve the results of purifying routes and controlling routes.

Examples

```
DGS-3610(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.

Platform description

30.1.51 neighbor route-reflector-client

This command configures the local device as the route reflector and specifies its client. The **no** form of the command cancels the client configured.

neighbor *ip-address* **route-reflector-client**

no neighbor *ip-address* **route-reflector-client**

Parameter description

Parameter	Description
ip address	Specify the address of the peer.

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

By default, all IBGP speakers in the autonomous system must establish the full neighboring relationship. The BGP speaker does not forward the routes learnt from a IBGP peer to the other IBGP peers, to prevent the occurring of 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 learnt IBGP route to the other IBGP peers.

Examples

```
DGS-3610(config)# router bgp 65000
DGS-3610(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

Platform description	

30.1.52 neighbor send-community

This command enables transmitting the community attributes to the specified BGP neighbor. You can use the **no** form of the command to disable this function.

neighbor {*ip-address* | *peer-group-name*} **send-community**

[**both** | **standard** | **extended**]

no neighbor {*ip-address* | *peer-group-name*} **send-community**

[**both** | **standard** | **extended**]

Parameter description

Parameter	Description
ip addres	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
both	Transmission for both standard and extended communities
standard	Transmission for the standard community only
extended	Transmission for the extended community only

Default configuration	Disabled.
Command mode	BGP configuration mode.
Usage guidelines	This command allows transmitting the specified attribute of the community to the fixed neighbor or a group of neighbor.
Examples	`DGS-3610(config-router)# neighbor ip-address 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

Platform description

30.1.53 neighbor shutdown

This command closes the BGP connection established with the specified BGP peer. The **no** form of the command restarts the BGP peer (group).

neighbor {*ip-address* | *peer-group-name*} **shutdown**

no neighbor {*ip-address* | *peer-group-name*} **shutdown**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command is used to close 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

```
DGS-3610(config)# router bgp 60
DGS-3610(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.

Platform description	

30.1.54 neighbor soft-reconfiguration inbound

This command allows storing the routing information sent from the BGP peer. Use the **no** form of the command to disable them.

neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**

no neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**

Parameter description	**Parameter**	**Description**
	ip address	Specify the peer address.
	peer-group-name	Specify the name of the peer group. The name of the peer group is within 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 route refreshing function, this command becomes unnecessary. You may run the **show ip bgp neighbors** command to judge whether the peer can support the route refreshing 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.55 neighbor timers

In specifying the BGP peer to establish the BGP connection, this command is used to set the *keepalive* and *holdtime* time values used for establishing the BGP connection. Use the **no** form of the command to restore the default setting.

neighbor [*ip-address* | *peer-group-name*] **timers** *keepalive holdtime*

no neighbor [*ip-address* | *peer-group-name*] **timers** *keepalive holdtime*

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
keepalive	Time interval of sending the KEEPALIVE message to the BGP peer. Range: 0-65535 seconds.
holdtime	Time interval of considering the BGP peer alive. Range: 0-65535 seconds.

Default configuration

keepalive: 60 seconds

holdtime: 180 seconds

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

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor 10.0.0.1 80 240
```

Related commands

Command	Description
router bgp	Enable the BGP protocol
timers bgp	Set the *keepalive* and *holdtime* values globally.

Platform description

30.1.56 neighbor unsuppress-map

This command allows selectively advertising the routing information that has been suppressed with the **aggregate-address** command. Use the **no** form of the command to restore the default setting.

neighbor {*ip-address* | *peer-group-name*} **unsuppress-map** *map-tag*

no neighbor {*ip-address* | *peer-group-name*} **unsuppress-map**

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32 characters
map-tag	Name of the route-map. Name of route map is up to 32 characters.

Default configuration

Disabled.

Command mode	BGP configuration mode.
Usage guidelines	This command allows advertising 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	`DGS-3610(config)# router bgp 65000` `DGS-3610(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

Platform description

30.1.57 neighbor update-source

In specifying the BGP peer to establish the BGP connection, this command is used to set the network interface used for establishing the BGP connection. The **no** form of the command automatically matches the optimal local interface.

neighbor {*ip-address* | *peer-group-name*} **update-source**

interface-type interface-index

no neighbor {*ip-address* | *peer-group*-name} **update-source**

interface-type interface-index

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 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.

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

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.58 neighbor version

This command shows 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** *numbe*r

Parameter description

Parameter	Description
ip address	Specify the peer address.
peer-group-name	Specify the name of the peer group. The name of the peer group is within 32

	characters
number	Version Number.

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

```
DGS-3610(config-router)# neighbor ip-address version 3
```

Related commands

Command	Description
router bgp	Enable the BGP protocol
neighbor remote-as	Configure the BGP peer.

Platform description

30.1.59 network(BGP)

This command configures 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. The name of route map is no more than 32 characters.
backdoor	The route is a backdoor route.

Default

The network information is not specified.

configuration	
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	`DGS-3610(config)# router bgp 65000` `DGS-3610(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	Synchronization switch of the network configuration network segment

Platform description	

30.1.60 network synchronization

This command configures advertising the network information of the network configuration after the local BGP speaker is synchronized with the local router. The **no** form of the command directly advertises the network information of the network configuration.

network synchronization

no network synchronization

Parameter description	None
Default configuration	The **network** information synchronization is turned on.
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

```
DGS-3610(config)# router bgp 65000
DGS-3610(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.

Platform description

30.1.61 redistribute

This is the route redistributing command, which redistributes the routing information between the other routing protocol and the BGP. The **no** form of the command deletes the function and the parameter configurations.

redistribute *protocol-type* [**route-map** *map-tag*]

no redistribute *protocol-type* [**route-map** *map-tag*]

Parameter description

Parameter	Description
protocol-type	The source protocol types for redistributing routes include Connected, Static, Rip, Ospf and isis
route-map *map-tag*	The name of the relevant **route-map**. None connected with **route-map** by default.

Default configuration

Disabled by default.

Command mode

BGP 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. The switches can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

Examples

```
DGS-3610(config-router)# redistribute static route-map static-rmap
DGS-3610(config-router)# no redistribute static
route-map static-rmap
DGS-3610(config-router)# no redistribute static
```

Related commands

Command	Description
show ip protocol	Show the protocol configuration.

Platform description

30.1.62 router bgp

Turn on the BGP protocol, configure the local autonomous system number and enter the BGP protocol configuration mode. The **no** form of the command turns off the BGP protocol.

router bgp *as-number*

no router bgp *as-number*

Parameter description

Parameter	Description
as-number	AS number. Range: 1 to 65535

Default configuration

BGP protocol is desabled by default.

Command mode

Global configuration mode.

Usage guidelines

This command is used to start the BGP protocol.

Examples

```
DGS-3610(config)# router bgp 65000
```

Related commands

Command	Description
ip routing	Enable IP routing

	bgp router-id	Set the identifier used to run the BGP protocol
	network	Set the network information to be advertised by the local BGP speaker.

Platform description

30.1.63 synchronization

This command starts the synchronization mechanism of the BGP and IGP routing information. The **no** form of the command cancels the synchronization mechanism of the BGP and IGP routing information.

synchronization

no synchronization

Parameter description

This command has no parameters.

Default configuration

The synchronization is turned off by default.

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 route information which passes through this AS (In general, this AS is an end AS).
2. All routers 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

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# synchronization
```

Related

Command	Description

commands	**router bgp**	Enable the BGP protocol

Platform description

30.1.64 timers bgp

This command is used 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

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

```
DGS-3610(config)# router bgp 65000
DGS-3610(config-router)# neighbor 10.0.0.1 80 240
```

Related commands

Command	Description
neighbor timers	Set the *keepalive* and *holdtime* values on the basis of neighbors

Platform description

30.2 Showing Related Command

30.2.1 show bgp ipv4 unicast

This command is used to show the IPv4 unicast routing information in the BGP routing information.

show bgp ipv4 unicast [{**network** | *network-mask*}]

Parameter description

Parameter	Description
network	Show the specific routing information in the routing table
network-mask	Show the routing information included in the specified network.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to view the BGP IPv4 unicast routing information.

Examples

```
DGS-3610# show bgp ipv4 unicast
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
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
```

Related commands

Platform description

30.2.2 show bgp ipv4 unicast community

This command is used to show the BGP IPv4 unicast routing information that contains a specific **community** value.

show bgp ipv4 unicast community *community-number* [**exact -match**]

Parameter description

Parameter	Description
community-number	Community number, in the form of AA:NN (autonomous system number/2-byte numeral), or any of the following predefined values: internet, no-export, local-as, no-advertise
exact -match	Show the routing information that fully matches the community value.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the IPv4 unicast routing information with specified **community** value.

Examples

```
DGS-3610# show bgp ipv4 unicast community local-as 111:12345
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
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
```

Related commands

Platform

description

30.2.3 show bgp ipv4 unicast community-list

This command is used to show the BGP IPv4 unicast routing information that matches specified community list.

show bgp ipv4 unicast community-list *community-name* [**exact-match**]

Parameter description

Parameter	Description
community-name	Name of the community list
exact -match	Routing information fully matching the community list

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to view the information of the community list with BGP configured.

Examples

```
DGS-3610# show bgp ipv4 unicast community-list my-comm
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
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
```

Related commands

Command	Description
ip community-list	Define the community list

Platform description

30.2.4 show bgp ipv4 unicast dampening dampened-paths

This command is used to show the suppressed IPv4 unicast path.

show bgp ipv4 unicast dampening dampened-paths

Parameter description	This command has no parameters.
Default configuration	No default configuration.
Command mode	Privileged mode.
Usage guidelines	This command is used to show the suppressed IPv4 unicast path.
Examples	DGS-3610# **show bgp ipv4 unicast dampening dampened-paths** Status codes: s suppressed, d damped, h history, * valid, > best, i - internal Origin codes: i - IGP, e - EGP, ? - incomplete Network From Reuse Path *d 192.168.64.0/24 110.110.110.10 00:21:41 1000 i *d 202.117.121.0/24 110.110.110.10 00:21:43 1000 ? *d 202.117.122.0/23 110.110.110.10 00:21:43 1000 ? *d 202.117.122.0/23 110.110.110.10 00:21:43 1000 ? *d 202.117.122.0/23 110.110.110.10 00:21:43 1000 ? *d 202.117.122.0/23 110.110.110.10 00:21:43 1000 ? *d 202.117.122.0/23 110.110.110.10 00:21:43 1000 ? *d 202.117.122.0/23 110.110.110.10 00:21:43 1000 ? *d 202.117.122.0/23 110.110.110.10 00:21:43 1000 ?
Related commands	
Platform description	

30.2.5 show bgp ipv4 unicast dampening flap-statistics

This command is used to show the IPv4 unicast route dampening statistics.

show bgp ipv4 unicast dampening flap-statistics

Parameter description	This command has no parameters.
Default configuration	No default configuration.
Command mode	Privileged mode.
Usage guidelines	This command is used to show the BGP IPv4 unicast route dampening statistics.
Examples	DGS-3610# **show bgp ipv4 unicast dampening flap-statistics** Status codes: s suppressed, d damped, h history, * valid, > best, i - internal Origin codes: i - IGP, e - EGP, ? - incomplete Network From Flaps Duration Reuse Path h 192.168.64.0/24 110.110.110.10 2 00:19:17 1000 i h 201.234.1.0/24 110.110.110.10 2 00:19:17 1000 ? h 201.234.2.0/23 110.110.110.10 2 00:19:17 1000 ? h 201.234.2.0/23 110.110.110.10 2 00:19:17 1000 ? h 201.234.2.0/23 110.110.110.10 2 00:19:17 1000 ? h 201.234.2.0/23 110.110.110.10 2 00:19:17 1000 ?
Related commands	
Platform description	

30.2.6 show bgp ipv4 unicast dampening parameters

This command is used to show the route dampening parameters configured for the BGP.

show bgp ipv4 unicast dampening parameters

Parameter description	This command has no parameters.
Default configuration	No default configuration.

Command mode	Privileged mode
Usage guidelines	This command is used to show the route dampening parameters configured for the BGP.

Examples	`DGS-3610(config-router)# bgp dampening 25 10000 10000 200`
	`DGS-3610# 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`

Related commands	
Platform description	

30.2.7 show bgp ipv4 unicast filter-list

This command is used to show the routing information that matches the filtering list.

show bgp ipv4 unicast filter-list *path-list-number*

Parameter description

Parameter	Description
path-list-number	Filtering list identifier

Default configuration	No default configuration.
Command mode	Privileged mode.
Usage guidelines	This command is used to show the routing information that matches the filtering list.

Examples

```
DGS-3610(config)# ip as-path access-list 5 permit .*
DGS-3610# show bgp ipv4 unicast filter-list 5
BGP table version is 1, local router ID is 192.168.88.200
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 Weight Path
*> 192.168.88.0    0.0.0.0                      32768 ?
Total number of prefixes 1
```

Related commands

Platform description

30.2.8 show bgp ipv4 unicast inconsistent-as

This command is used to show the IPv4 unicast route information of inconsistent source AS.

show bgp ipv4 unicast inconsistent-as

Parameter description This command has no parameters.

Default configuration No default configuration.

Command mode Privileged mode.

Usage guidelines This command is used to show the IPv4 unicast routing information of inconsistent source AS.

Examples

```
DGS-3610# show bgp ipv4 unicast inconsistent-as
```

Related commands

Platform

description	

30.2.9 show bgp ipv4 unicast neighbors

This command is used to show the related information of BGP neighbor.

show bgp ipv4 unicast neighbors [*neighbor-address*]

[**received-routes | routes | advertised-routes**]

Parameter description

Parameter	Description
neighbor-address	Specify the address for a peer.
received-routes	Show all routing information received from the peer (including the accepted routes and rejected routes).
routes	Show all routes that come from the peer and are accepted.
advertised-routes	Show all sent route information.

Command mode	Privileged mode.

Usage guidelines	This command is used to view the information of the connection with BGP neighbor.

Examples

```
DGS-3610# show bgp ipv4 unicast neighbors
BGP neighbor              : 12.12.12.2
Remote AS                 : 100
Local AS                  : 100
Neighbor type             : internal
BGP version               : 4
Remote ID                 : 192.168.4.2
BGP state                 : Established, up for 00:53:30
Min advertisement interval(secs): 15
Configured holdtime       : 90
Configured keepalive      : 30
Hold time                 : 90
keepalive                 : 30
Neighbor capabilities     : ignore
Address family IPv4 Unicast: advertised , recieved
Route refresh             : advertised , recieved
Connections established   : 1
Connections dropped       : 0
Last reset                : never
Local  host               : 12.12.12.1  Local port  : 179
```

```
Remote host              : 12.12.12.2  Remote port : 1067
Maximum-Prefix limit     : 4294967295
Threshold for warning    : 0%
Accepted prefixes        : 0
Prefix advertised        : 6
Received messages        : 110
Sent messages            : 116
Received notifications   : 0
Sent notifications       : 0
Route refresh received   : 0
Route refresh sent       : 0
DGS-3610# show bgp ipv4 unicast neighbors 15.15.15.5 routes
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network  Next Hop         Metric           LocPrf     Path
*>i   58.1.1.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.2.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.3.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.4.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.5.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.6.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.7.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.8.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.9.0/24       58.58.58.8          58     100 800 ?
*>i   58.1.10.0/24      58.58.58.8          58     100 800 ?
*>i   67.1.1.0/24       67.67.67.7          67     100 700 ?
*>i   67.1.2.0/24       67.67.67.7          67     100 700 ?
*>i   67.1.3.0/24       67.67.67.7          67     100 700 ?
*>i   67.1.4.0/24       67.67.67.7          67     100 700 ?
*>i   67.1.5.0/24       67.67.67.7          67     100 700 ?
*>i   67.1.6.0/24       67.67.67.7          67     100 700 ?
```

Related commands

Platform description

30.2.10 show bgp ipv4 unicast paths

This command is used to show the path information of IPv4 unicast in the route database.

show bgp ipv4 unicast paths

Parameter description	This command has no parameters.
Command mode	Privileged mode.
Usage guidelines	This command is used to view the path information in the route database.
Examples	`DGS-3610# show bgp ipv4 unicast paths`
Related commands	
Platform description	

30.2.11 show bgp ipv4 unicast quote-regexp

This command is used to show the BGP routing information that the AS path attribute matches the regular expression in the specified double quotation marks.

show bgp ipv4 unicast quote-regexp *regexp*

Parameter description

Parameter	Description
regexp	Regular expression for matching AS path attributes, with comma included.

Default configuration	No default configuration.
Command mode	Privileged mode.
Usage guidelines	This command is used to show the BGP routing information that the AS path attribute matches the regular expression in the specified double quotation marks. Note that the regular expression shall be enclosed with double quotation marks.

Examples

```
DGS-3610# show bgp ipv4 unicast quote-regexp "_300_"
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
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
```

Related commands

Platform description

30.2.12 show bgp ipv4 unicast regexp

This command is used to show the BGP routing information that the AS path attribute matches the specified regular expression.

show bgp ipv4 unicast regexp *regexp*

Parameter description

Parameter	Description
regexp	Regular expression for matching AS path attributes

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the BGP routing information that the AS path attribute matches the specified regular expression.

Examples

```
DGS-3610# show bgp ipv4 unicast regexp _300_
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
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
```

Related commands

Platform description

30.2.13 show bgp ipv4 unicast summary

Use this command to show the relevant information of BGP.

show bgp ipv4 unicast summary

Parameter description

This command has no parameters.

Command mode

Privileged mode.

Usage guidelines

Use this command to view the relevant information of BGP.

Examples

```
DGS-3610# show bgp ipv4 unicast summary
BGP router identifier 192.168.88.200, local AS number 500
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries
Neighbor   V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
1.1.1.1    4   200     0      0      0    0    0    never Active
Total number of neighbors 1
```

Related commands

Command	Description
router bgp	Enable the BGP protocol

Platform description

30.2.14 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	Show 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

No default configuration.

Command mode

Privileged mode.

Usage guidelines

Use this command to view the route information of BGP.

Examples

```
DGS-3610# 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
```

Related commands

Platform description

30.2.15 show ip bgp cidr-only

This command shows unclassified routes.

show ip bgp cidr-only

Parameter description	This command has no parameters.
Default configuration	No default configuration.
Command mode	Privileged mode.
Usage guidelines	This command is used to view the unclassified routing information.
Examples	`DGS-3610# show ip bgp cidr-only`

Related commands

Command	Description
bgp dampening	Turn on the route dampening function and set the dampening parameters.
clear ip bgp dampening	Clear the suppressed routes.

Platform description

30.2.16 show ip bgp community

This command is used to show the BGP routing information with specified community value.

show ip bgp community *community-number* [**exact -match**]

Parameter description

Parameter	Description
community-number	Community number, in the form of AA:NN (autonomous system number/2-byte numeral), or any of the following predefined values: internet, no-export, local-as, no-advertise
exact -match	Show the routing information that fully matches the community value**.**

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the routing information with specified **community** value.

Examples

```
DGS-3610# show ip bgp community local-as 111:12345
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
```

Related commands

Platform description

30.2.17 show ip bgp community-list

This command is used to show the BGP routing information that matches specified community list.

show ip bgp community-list *community-name* [**exact-match**]

Parameter description

Parameter	Description
community-name	Name of the community list
exact-match	Routing information fully matching the community list

Default configuration

No default configuration.

Command mode

Privileged mode

Usage guidelines

This command is used to view the information of the community list with BGP configured.

Examples

```
DGS-3610# show ip bgp community-list my_comm
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
```

Related commands

Command	Description
ip community-list	Define the community list.

Platform description

30.2.18 show ip bgp dampening dampened-paths

This command is used to show the suppressed path.

show ip bgp dampening dampened-paths

Parameter description

This command has no parameters.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the suppressed path.

Examples

```
DGS-3610# show ip bgp dampening dampened-paths
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
status Network          From          Reuse    Path
------ ---------- ---------- -------- --------------
*d    192.168.64.0/24   110.110.110.10  00:21:41 1000 i
*d    202.117.121.0/24  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
```

Related commands

Platform description

30.2.19 show ip bgp dampening flap-statistics

This command is used to show the route dampening statistics.

show ip bgp dampening flap-statistics

Parameter description This command has no parameters.

Default configuration No default configuration.

Command mode Privileged mode.

Usage guidelines This command is used to show the BGP route dampening statistics.

Examples

```
DGS-3610# show ip bgp dampening flap-statistics
Status codes: s suppressed, d damped, h history, * valid, > best,
```

```
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network        From        Flaps  Duration Reuse    Path
------ --------- ---------- ------ -------- -------- ------------
h     192.168.64.0/24   110.110.110.10    2 00:19:17      1000 i
h     201.234.1.0/24    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
```

Related commands

Platform description

30.2.20 show ip bgp dampening parameters

This command is used to show the route dampening parameters configured for the BGP.

show ip bgp dampening parameters

Parameter description

This command has no parameters.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the route dampening parameters configured for the BGP.

Examples

```
DGS-3610(config-router)# bgp dampening 25 10000 10000 200
DGS-3610# show ip bgp 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
```

Related commands

Platform description

30.2.21 show ip bgp filter-list

This command is used to show the routing information that matches the filtering list.

show ip bgp filter-list *path-list-number*

Parameter description

Parameter	Description
path-list-number	Filtering list identifier

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the routing information that matches the filtering list.

Examples

```
DGS-3610(config)# ip as-path access-list 5 permit .*
DGS-3610# show ip bgp filter-list 5
BGP table version is 1, local router ID is 192.168.88.200
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 Weight Path
*> 192.168.88.0    0.0.0.0                          32768 ?
Total number of prefixes 1
```

Related commands

Platform description

30.2.22 show ip bgp inconsistent-as

This command is used to show the route information of inconsistent source AS.

show ip bgp inconsistent-as

Parameter description This command has no parameters.

Default configuration No default configuration.

Command mode Privileged mode.

Usage guidelines This command is used to show the routing information of inconsistent source AS.

Examples

```
DGS-3610# show ip bgp inconsistent-as
```

Related commands

Platform description

30.2.23 show ip bgp neighbors

This command is used to show the related information of BGP neighbor.

show ip bgp neighbors [*neighbor-address*] [**received-routes | routes | advertised-routes**]

Parameter description

Parameter	Description
neighbor-address	Specify the address for a peer.
received-routes	Show all routing information received from the peer (including the received routes and rejected routes).
routes	Show all routes that come from the peer and

	are accepted.
advertised-routes	Show all sent route information.

Command mode

Privileged mode.

Usage guidelines

This command is used to view the information of the connection with BGP neighbor.

Examples

```
DGS-3610# show ip bgp neighbors
BGP neighbor                : 12.12.12.2
Remote AS                   : 100
Local AS                    : 100
Neighbor type               : internal
BGP version                 : 4
Remote ID                   : 192.168.4.2
BGP state                   : Established, up for 00:53:30
Min advertisement interval(secs): 15
Configured holdtime         : 90
Configured keepalive        : 30
Hold time                   : 90
keepalive                   : 30
Neighbor capabilities       : ignore
Address family IPv4 Unicast : advertised , recieved
Route refresh               : advertised , recieved
Connections established     : 1
Connections dropped         : 0
Last reset                  : never
Local  host                 : 12.12.12.1  Local port  : 179
Remote host                 : 12.12.12.2  Remote port : 1067
Maximum-Prefix limit        : 4294967295
Threshold for warning       : 0%
Accepted prefixes           : 0
Prefix advertised           : 6
Received messages           : 110
Sent messages               : 116
Received notifications      : 0
Sent notifications          : 0
Route refresh received      : 0
Route refresh sent          : 0
DGS-3610# show ip bgp neighbors 15.15.15.5 routes
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
```

```
------ ----------- ----------- -------- -------- -----------
*>i    58.1.1.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.2.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.3.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.4.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.5.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.6.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.7.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.8.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.9.0/24       58.58.58.8          58     100 800 ?
*>i    58.1.10.0/24      58.58.58.8          58     100 800 ?
*>i    67.1.1.0/24       67.67.67.7          67     100 700 ?
*>i    67.1.2.0/24       67.67.67.7          67     100 700 ?
*>i    67.1.3.0/24       67.67.67.7          67     100 700 ?
*>i    67.1.4.0/24       67.67.67.7          67     100 700 ?
*>i    67.1.5.0/24       67.67.67.7          67     100 700 ?
*>i    67.1.6.0/24       67.67.67.7          67     100 700 ?
```

Related commands

Platform description

30.2.24 show ip bgp paths

This command is used to show the path information in the route database.

show ip bgp paths

Parameter description This command has no parameters.

Command mode Privileged mode.

Usage guidelines This command is used to view the path information in the route database.

Examples

```
DGS-3610# show ip bgp paths
```

Related

commands

Platform description

30.2.25 show ip bgp quote-regexp

This command is used to show the BGP routing information that the AS path attribute matches the regular expression in the specified double quotation marks.

show ip bgp quote-regexp *regexp*

Parameter description

Parameter	Description
regexp	Regular expression for matching AS path attributes, with comma included.

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the BGP routing information that the AS path attribute matches the regular expression in the specified double quotation marks.

Note that the regular expression shall be enclosed with double quotation marks.

Examples

```
DGS-3610# show ip bgp quote-regexp "_300_"
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
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
```

Related commands

Platform

description

30.2.26 show ip bgp regexp

This command is used to show the BGP routing information that the AS path attribute matches the specified regular expression.

show ip bgp regexp *regexp*

Parameter description

Parameter	Description
regexp	Regular expression for matching AS path attributes

Default configuration

No default configuration.

Command mode

Privileged mode.

Usage guidelines

This command is used to show the BGP routing information that the AS path attribute matches the specified regular expression.

Examples

```
DGS-3610# show ip bgp regexp _300_
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
```

Related commands

Platform description

30.2.27 show ip bgp summary

This command is used to show the related information of BGP.

show ip bgp summary

Parameter description	This command has no parameters.
Command mode	Privileged mode.
Usage guidelines	This command is used to show the related information of BGP.

Examples

```
DGS-3610# show ip bgp summary
BGP router identifier 192.168.88.200, local AS number 500
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
1.1.1.1     4   200      0      0       0    0    0    never Active
Total number of neighbors 1
```

Related commands

Command	Description
router bgp	Enable the BGP protocol

Platform description

30.2.28 show ip community-list

This command is used to show the related information of community list.

show ip community-list [*community-list-number*|*community-list-name*]

Parameter description

Parameter	Description
community-list-number	Number of the community to display the information
community-list-name	Name of the community to display the information

Default configuration No default configuration.

Command mode	Privileged mode
Usage guidelines	This command is used to view the related information of community list.
Examples	DGS-3610# **show ip community-list** Community-list standard local permit local-AS Community-list standard D-Link permit 0:10 deny 0:20
Related commands	
Platform description	

30.2.29 show ip as-path-access-list

This command is used to show the related information of community list.

show ip as-path-access-list {*num*}

Parameter description

Parameter	Description
num	as-path-access-list number to display the information

Default configuration	No default configuration.
Command mode	Privileged mode.
Usage guidelines	This command is used to view the **as-path-access-list** information.
Examples	DGS-3610# **show ip as-path-access-list** AS path access list 30 permit ^30$

Related commands

Platform description

31 Protocol-independent Command Reference

31.1 Configuration Related Commands

31.1.1 distribute-list in

Use this command to control the route update processing in order to filter routes. Use the **no** form of this command to delete 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	Set the access list. 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.
i*nterface-type interface-number*	(Optional) Use the distribution list in on the specified interfaces.

Default configuration

No distribution list is defined.

Command mode

Routing process configuration mode.

Usage guidelines

To reject some specified routes, you can configure the route distribution list to process all the received route update messages. This command does not applies to the OSPF routing protocol, because the OSPF receives link state description 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 controls 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	Sets the access list.
prefix-list	Sets the prefix list.

Platform description

Version description

31.1.2 distribute-list out

Use this command to control the route update advertisement for the purpose of route filtering. Use the **no** form of this command to delete the setting.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id*]

Parameter description

Parameter	Description
access-list-number	Set the access list. Only the routes permitted in the access list can be transmitted.
prefix *prefix-list-name*	Use the prefix list to filter routes.
interface	(Optional) Only the route update advertisements of the specified interface are controlled.

	protocol	(Optional) The routes of the specified routing protocol are redistributed.

Default configuration

Not configured.

Command mode

Routing process configuration mode.

Usage guidelines

If no optional parameter is used in this command, the route update advertisement of all the interfaces is controlled. If the interface option is used, only the route update advertisement of the specified interface is controlled. If other routing process parameters used, the routes of the specified routing process are filtered for redistribution.

The route update advertisement control in the OSPF routing process applies only to the external routes of the OSPF AS, and no interface shall be specified.

Examples

The following example enables the advertisement of 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	Sets the access list.
prefix-list	Sets the prefix list.
redistribute	Configures the route redistribution.

31.1.3 match as-path

To redistribute the AS_PATH attribute route allowed in the access list, use the route map configuration command **match as-path**. Use the **no** form of this command to delete the setting.

match as-path { *access-list-number* | *access-list-name*}

no match as-path { *access-list-number* | *access-list-name*}

Parameter description

Parameter	Description
access-list-number	Number of the access list.
access-list-name	Name of the access list.

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

The "match as-path" can be followed by an access list number or name.

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

```
!
route-map IGP2BGP
match as-path 20
```

Related commands

Command	Description
match community	Match route community value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.

31.1.4 match community

To redistribute the COMMUNITY attribute route allowed in the access list, use the route map configuration command **match community**. Use the **no** form of this command to delete the setting.

match community { *community-list-number* | *community-list-name*}

[*exact-match*]

no match community {*community-list-number* | *community-list-name*}

[*exact-match*]

Parameter description

Parameter	Description
community-list-number	Community list number
communitys-list-name	Community list name
exact-match	Exact match list.

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

The **"match community**" can be followed by a community list number or name.

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

```
ip community-list 1 permit 109
!
route-map set_weight
match community 1 exact
set weight 200
```

Related commands

Command	Description
match as-path	Match route AS_PATH attribute value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.

31.1.5 match interface

Use this command to redistribute the route as the specified next-hop interface. Use the **no** form of this command to delete 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

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

Multiple interfaces may follow **match interface**.

To enable the router to run multiple routing protocol processes, DGS-3610 series 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 on the 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 address in the access list.
match ip route-source	Match the route source address in the 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.

Platform description

Version description

31.1.6 match ip address

Use this command to redistribute the network routes permitted in the access list. Use the **no** form of this command to delete the setting.

match ip address { *access-list-number* | *access-list-name*}

[*... access-list-number* | *... access-list-name*]

no match ip address { *access-list-number* | *access-list-name*}

[*... access-list-number* | *... access-list-name*]

Parameter description

Parameter	Description
access-list-number	Number of the access list.
access-list-name	Name of the access list.

Default configuration

No default configuration.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow **match ip address**.

To enable the router to run multiple routing protocol processes, DGS-3610 series 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 on the 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 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.

Platform description

Version description

31.1.7 match ip next-hop

Use this command to redistribute the network routes whose next-hop IP address matches the access list. Use the **no** form of this command to delete the setting.

match ip next-hop { *access-list-number* | *access-list-name*}

[*... access-list-number* | *... access-list-name*]

no match ip next-hop { *access-list-number* | *access-list-name*}

[*... access-list-number* | *... access-list-name*]

Parameter description

Parameter	Description
access-list-number	Number of the access list.

access-list-name	Name of the access list.

Default configuration

No default configuration.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow **match ip next-hop**.

To enable the router to run multiple routing protocol processes, DGS-3610 series 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. As long as the next hop address of the RIP route matches access list 10 or 20, the OSPF allows the redistributing.

```
!
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 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 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.

Platform description

Version description

31.1.8 match ip route-source

Use this command to redistribute the network routes whose next-hop IP address matches the access list. Use the **no** form of this command to delete the setting.

match ip route-source { *access-list-number* | *access-list-name*}

[*... access-list-number* | *... access-list-name*]

no match ip route-source { *access-list-number* | *access-list-name*}

[*... access-list-number* | *... access-list-name*]

Parameter description

Parameter	Description
access-list-number	Number of the access list.
access-list-name	Name of the access list.

Default configuration Not configured.

Command mode Route map configuration mode.

Usage guidelines

Multiple access list numbers may follow **match ip route-source**.

To enable the router to run multiple routing protocol processes, DGS-3610 series 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. As long as the source IP address of the RIP route matches access list 5, the OSPF allows the redistributing.

```
!
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 address in 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 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.

Platform description

Version description

31.1.9 match metric

Use this command to redistribute the network routes with the specified metric. Use the **no** form of this command to delete the setting.

match metric *metric*

no match metric *metric*

Parameter description

Parameter	Description
metric	Route metric.

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

To enable the router to run multiple routing protocol processes, DGS-3610 series 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. Only for the RIP routes with metric 10, the OSPF allows the redistributing.

```
!
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 10

!
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the address in 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 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.

Platform description

Version description

31.1.10 match origin

To redistribute route of the origin allowed in the access list, use the route map configuration command **match origin**. Use the **no** form of this command to delete the setting.

match origin {**egp** | **igp** | **incomplete**}

no match origin {**egp** | **igp** | **incomplete**}

Parameter description

Parameter	Description
egp	The origin is the remote EGP.
igp	The origin is the local IGP.
Incomplete	The origin is unknown

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

This command is used to set the condition for matching the route origin.

Examples

```
route-map MY_MAP 10 permit
match origin egp
set community 109
!
route-map MAP20 20 permit
match origin incomplete
set community no-export
```

Related commands

Command	Description
match as-path	Match route AS_PATH attribute value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric for route redistribution.
set origin	Set the type for route redistribution.

31.1.11 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 { internal | external [type-1 | type-2] | local }

no match route-type { internal | external [type-1 | type-2] | local }

Parameter description

Parameter	Description
internal	Internal route in the OSPF routing domain.
external[type-1 | type-2]	External route in the OSPF routing domain.
local	Local route.

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

To enable the router to run multiple routing protocol processes, DGS-3610 series 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 the OSPF routes. The RIP 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

Command	Description

commands	**access-list**	Set the access list.
	match ip address	Match the address in 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 route metric.
	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.

Platform description	

Version description	

31.1.12 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	No default configuration.
Command mode	Route map configuration mode.
Usage guidelines	The tag value may follow **match tag**. To enable the router to run multiple routing protocol processes,

DGS-3610 series 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 the OSPF routes. The RIP redistributes only the routes with tag 50 or 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 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 route metric.
match ip next-hop	Match the next-hop address in the access list.
match route-type	Match the route type.
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.

Platform description

Version description

31.1.13 match length

To implement the policy-based routing based on the IP packet length, run the route map configuration command **match length**. The **no** form of this command is used to delete the existing definition.

match length *min-length max-length*

no match length *min-length max-length*

Parameter description

Parameter	Description
min-length	Minimum length of the IP packet
max-length	Maximum length of the IP packet

Default configuration

No default configuration.

Command mode

Route map configuration mode.

Usage guidelines

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 router will decide how to process the packets that need be routed according to the route map, which decides the next-hop router 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.

To implement multiple paths for interactive traffic and large batch traffic, it is possible to use policy-based routing that is based on the packet size.

Examples

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic with packet size smaller than 500 bytes through fastethernet 1/0 interface.

```
interface fastethernet 1/0
ip policy route-map smallpak

route-map smallpak permit 10
match length 0 500
set interface fastethernet 0/0
```

Related commands

Command	Description
route-map	Define the route map
match ip address	Match the address in the access list
set default interface	Set the default packet output interface.
set interface	Set the packet output interface
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets
set ip precedence	Set the priority of the packets.

31.1.14 route-map

Uses this command to enter the route map configuration mode and define route maps. Use the **no** form of this command to delete 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	Set the name of the route map. The **redistribute** command references the route map according to its name. Multiple route map policies can be defined in a route map, and each policy corresponds to one sequence number.
permit	(Optional) If the “deny” keyword is used 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 used but the rule defined by **match** is not met,it enters the second route map and starts operation, till the **set** command is executed finally.
	deny	(Optional) If the “deny” keyword is used and the rule defined by **match** is met, no operation will be performed, and neither route redistribution nor policy-based routing is supported in the route map, and the route map operation is exited. If the “deny” keyword is used but the rule defined by **match** is not met, it enters the second route map and starts operation, 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 execute caution when setting the sequence number.

Default configuration	No route map is configured by default.
Command mode	Global configuration mode.
Usage guidelines	At present, the route maps of DGS-3610 series are primarily used for: 1. route redistribution control; 2. policy-based routing. 1. Route redistribution control To enable the router to run multiple routing protocol processes, DGS-3610 series 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.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

1) In creating 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.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the redistribution next hop count of 4, with the type being type-1, the default metric being 40 and the tag being 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	Implement route redistribution.

Platform description

Version description

31.1.15 set as-path prepend

To specify the AS_PATH attribute value for the route that match the rule, use the route map configuration command **set as-path prepend**. Use the **no** form of this command to delete the setting. This command is only used to configure routing policies.

set as-path prepend *as-number*

no set as-path prepend *as-number*

Parameter description

Parameter	Description
as-number	AS number to add the AS_PATH attribute

Default configuration

No default configuration.

Command mode

Route map configuration mode.

Usage guidelines

This command is used to set the prepared AS_PATH attribute for the matched route.

Examples

```
!
route-map set-as-path
match as-path 1
set as-path prepend 100 100 100
```

Related commands

Command	Description
match as-path	Match route AS_PATH value
match community	Match route community value
match metric	Match the route metric.
match origin	Match route origin value
set community	Set the COMMUNITY attribute of the redistributed routes
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.

31.1.16 set community

To specify the COMMUNITY attribute value for the route that match the rule, use the route map configuration command **set community**. Use the **no** form of this command to delete the setting. This command is only used to configure routing policies.

set community *community-number* [**additive** | **none**]

no set community *community-number* [**additive** | **none**]

Parameter description

Parameter	Description
community-number	Community number, Format: AA:NN. In addition, it can be known community attribute internet, local-AS, no-export or no-advertise.
additive	Add to the original attribute.
none	Set the community attribute as blank.

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

This command is used to set the community attribute for the matched route.

Examples

```
route-map SET_COMMUNITY 10 permit
match as-path 1
set community 109
!
route-map SET_COMMUNITY 20 permit
match as-path 2
set community no-export
```

Related commands

Command	Description
match as-path	Match route AS_PATH value
match community	Match route community value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set origin	Set the origin of redistributed routes
set metric-type	Set the type for route redistribution.

31.1.17 set comm-list delete

To delete the COMMUNITY_LIST attribute value for the route that matches the rule, use the route map configuration command **set comm.-list delete**. Use the **no** form of this command to delete the setting. This command is only used to configure routing policies.

set comm-list *community-list-number* | *community-list-name* **delete**

no comm-list *community-list-number* | *community-list-name* **delete**

Parameter description

Parameter	Description
community-list-number	Number of the community list
community-list-name	Name of the community list

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

This command is used to set the community list for the matched routes.

Examples

```
router bgp 100
neighbor 172.16.233.33 remote-as 120
neighbor 172.16.233.33 route-map ROUTEMAPIN in
neighbor 172.16.233.33 route-map ROUTEMAPOUT out
!
ip community-list 500 permit 100:10
ip community-list 500 permit 100:20
!
ip community-list 120 deny 100:50
ip community-list 120 permit 100:.*
!
route-map ROUTEMAPIN permit 10
set comm-list 500 delete
!
route-map ROUTEMAPOUT permit 10
set comm-list 120 delete
```

Related commands

Command	Description
match as-path	Match route AS_PATH attribute value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set local-preference	Set the local priority of redistributed routes

	set metric-type	Set the type for route redistribution.

31.1.18 set dampening

To specify the dampening parameters for the route that matches the rule, use the route map configuration command **set dampening**. Use the **no** form of this command to delete the setting. This command is only used to configure routing policies.

set dampening *half-life* [*reuse suppress max-suppress-time*]

no set dampening [*half-life*]

Parameter description

Parameter	Description
half-life	Half life in case of route reachable or unreachable. Range: 1-45 minutes, 15 minutes by default
reuse	When the route penalty is lower than this value, the route suppression is released. Range: 1 - 20000, 750 by default
suppress	When the route penalty is higher than this value, the route is suppressed. Range: 1 - 20000, 2000 by default
max-suppress-time	Maximum duration a route can be suppressed. Range: 1-20000 minutes, 4 half lives by default

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

This command is used to set the route dampening parameter for the matched route.

Examples

```
route-map tag
match as path 10
set dampening 30 1500 10000 120
!
router bgp 100
neighbor 172.16.233.52 route-map tag in
```

Related

Command	Description

commands	**match as-path**	Match route AS_PATH value
	match community	Match route community value
	match metric	Match the route metric.
	match origin	Match route origin value
	set as-path prepend	Set the AS_PATH attribute of redistributed routes
	set metric	Set the metric for route redistribution.
	set local-preference	Set the local priority of redistributed routes

31.1.19 set extcommunity

To specify the EXTCOMMUNITY attribute value for the route that matches the rule, use the route map configuration command **set extcommunity**. Use the **no** form of this command to delete the setting. This command is only used to configure routing policies.

set extcommunity {**rt** *extend-community-value* | **soo**

extend-community-value}

no set extcommunity {**rt** *extend-community-value* | **soo**

extend-community-value}

Parameter description

Parameter	Description
rt	Enter the extended community value in the form of RT
soo	Enter the extended community value in the form of SOO
extend-community-value	Extended community value

Default configuration	Not configured.
Command mode	Route map configuration mode.
Usage guidelines	This command is used to set the extended community attribute for the matched route.
Examples	`access-list 2 permit 192.168.78.0 255.255.255.0` `route-map MAP_NAME permit 10`

```
match ip-address 2
set extcommunity rt 100:2
```

Related commands

Command	Description
match as-path	Match route AS_PATH value
match community	Match route community value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.

31.1.20 set next-hop

Use this command to specify the next-hop IP address for the routes that meet the matching rule. Use the **no** form of this command to delete the setting. This command is only used to configure routing policies.

set next-hop *ip-address*

no set next-hop *ip-address*

Parameter description

Parameter	Description
ip address	IP address of the next hop.

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

To enable the router to run multiple routing protocol processes, DGS-3610 series 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.

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
!
route-map redrip permit 10
set next-hop 192.168.1.2
```

Related commands

Command	Description
match interface	Match the next-hop interface of the route.
match ip address	Match the address in the access list.
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 route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

31.1.21 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 delete the setting. This command is only used to configure routing policies.

set ip next-hop *ip-address* [*weight*] [*…ip-address*]

no set ip next-hop *ip-address* [*weight*] [*…ip-address*]

Parameter description

Parameter	Description
ip address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration

No default configuration.

Command mode

Route map configuration mode.

Usage guidelines

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.

Up to 32 IP addresses may follow **set ip next-hop**.

If weight follows **ip address**, up to 4 nexthop addresses can be configured.

Note: 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, if the **weight** of a **nexthop** address is configured, it is 1 by default.

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 router will decide how to process the packets that need be routed according to the route map, which decides the next-hop router 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, which are usually in this order:

- **set ip next-hop**

- **set interface**
- **set ip default next-hop**
- **set default interface**

Examples

The following example starts policy-based routing on serial 1/0. When the interface receives packets with the source network of 10.0.0.0, they will be sent to 192.168.100.1; when the interface receives packets with the source network of 172.16.0.0, they will be sent to 172.16.100.1; all other packets will be discarded.

```
interface serial 1/0
ip policy route-map load-balance

access-list 10 permit 10.0.0.0 0.255.255.255
access-list 20 permit 172.16.0.0 0.0.255.255

route-map load-balance permit 10
 match ip address 10
 set ip  next-hop 192.168.100.1
!
route-map load-balance permit 20
 match ip address 20
 set ip  next-hop 172.16.100.1
!
route-map load-balance permit 30
 set interface Null0
```

Related commands

Command	Description
route-map	Define the route map
match ip address	Match the address in the access list
set default interface	Set the default packet output interface.
set default interface	Set the default packet output interface.
set interface	Set the packet output interface
set ip default next-hop	Set the default next hop of the packets.
set ip precedence	Set the priority of the packets.

Platform description

Version description	

31.1.22 set level

To set the distributed interval type of the transmitted message IP header that matches the route map match rule, use the route map configuration command **set level**. Use the **no** form of this command to delete the setting.

set level {**level 1**| **level 2** | **level 1-2** | **stub-area** | **backbone**}

no set level

Default configuration	No default configuration.
Command mode	Route map configuration mode.
Usage guidelines	To enable the router to run multiple routing protocol processes, DGS-3610 series 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 protocol, and sets the distribution interval of the redistributed routes as the backbone interval.
	`!`
	`router ospf`
	`redistribute rip subnets route-map redrip`
	`network 192.168.12.0 0.0.0.255 area 0`
	`!`
	`!`
	`route-map redrip permit 10`
	`set level backbone`

Related commands

Command	Description
match interface	Match the next-hop interface of the route.
match ip address	Match the address in the access list.
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 route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

31.1.23 set local-preference

To set the LOCAL_PREFERENCE value of the redistributed routes, use the route map configuration command **set local-preference**. Use the **no** form of this command to delete the setting.

set local-preference *number*

no set local-preference *number*

Parameter description

Parameter	Description
number	Local priority metric. Range 1 - 4294967295, 100 by default

Default configuration

No default configuration.

Command mode

Route map configuration mode.

Usage guidelines

This command is used to set the local preference for the matched routes.

Examples

```
route-map SET_PREF 10 permit
match as-path 1
```

```
set local-preference 6800
!
route-map SET_PREF 20 permit
match as-path 2
set local-preference 50
```

Related commands

Command	Description
match as-path	Match route AS_PATH attribute value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.

31.1.24 set metric

Use this command to set the metric for the matching rule in the route map. Use the **no** form of this command to delete the setting.

set metric [+ *metric-value* | **-** *metric-value* | *metric-value*]

no set metric

Parameter description

	Parameter	Description
	+	Add (add to the metric of the original route)
	-	Decrease (decrease from the metric of the original route)
	Metric-value	Measurement for re-distribution route setting

Default configuration

The default metric for route redistribution varies with the routing protocol.

Command mode

Route map configuration mode.

Usage guidelines

Set the metric according to the actual network topology, because it affects the routing. Pay attention to the upper and lower limits of the routing protocols when running the **set metric**, **+ metric** or **– metric** commands. For the RIP protocol redistribution to other protocols, the

range of the result after adding or deleting metric is 1–16.

To enable the router to run multiple routing protocol processes, DGS-3610 series 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 routes and sets the default metric to 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
 set metric 40
```

Related commands

Command	Description
match interface	Match the next-hop interface of the route.
match ip address	Match the address in the access list.
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 route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

Platform

description

Version description

31.1.25 set metric-type

Use this command to set the type for the matching rule in the route map. Use the **no** form of this command to delete the setting.

set metric-type *type*

no set metric-type

Parameter description

Parameter	Description
type	Set the type for route redistribution. At present, the type for route redistribution can be set for OSPF only. type-1: Type 1 external route; type-2: Type 2 external route.

Default configuration

Type-2

Command mode

Route map configuration mode.

Usage guidelines

This command can only be used by the OSPF to redistribute other types of routes.

To enable the router to run multiple routing protocol processes, DGS-3610 series 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.

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
route-map redrip permit 10
 set metric-type type-1
```

Related commands

Command	Description
match interface	Match the next-hop interface of the route.
match ip address	Match the address in the access list.
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 route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set tag	Set the tag for route redistribution.

Platform description

Version description

31.1.26 set origin

To redistribute route of the origin allowed in the access list, use the route map configuration command **set origin**. Use the **no** form of this command to delete the setting.

set origin {**egp** | **igp** | **incomplete**}

no set origin {**egp** | **igp** | **incomplete**}

Parameter description

Parameter	Description
egp	The origin is the remote EGP.
igp	The origin is the local IGP.
Incomplete	The origin is unknown

Default configuration

Not configured.

Command mode

Route map configuration mode.

Usage guidelines

This command is used to set the origin for matching the routes.

Examples

```
route-map SET_ORIGIN 10 permit
match as-path 1
set origin igp
route-map SET_ORIGIN 20 permit
match as-path 2
set origin egp
```

Related commands

Command	Description
match as-path	Match route AS_PATH attribute value
match metric	Match the route metric.
match origin	Match route origin value
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric for route redistribution.
set local-preference	Set the local priority of redistributed routes

31.1.27 set tag

Use this command to sets the tag for route redistribution. Use the **no** form of this command to delete the setting.

set tag *tag*

no set tag

Parameter description

Parameter	Description
tag	Set the tag for route redistribution.

Default configuration

The original routing tag remains unchanged.

Command mode

Route map configuration mode.

Usage guidelines

This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

To enable the router to run multiple routing protocol processes, DGS-3610 series 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 tag as 100.

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
route-map redrip permit 10
 set tag 100
```

Related commands

Command	Description
match interface	Match the next-hop interface of the route.
match ip address	Match the address in the access list.

	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 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.

Platform description

Version description

31.1.28 set ip default 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 delete the setting.

set ip default next-hop *ip-address* [weight] […*ip-address*]

no set ip default next-hop *ip-address* [weight] […*ip-address*]

Parameter description

Parameter	Description
ip address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration

No default configuration.

Command mode

Route map configuration mode.

Usage guidelines

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.

Up to 32 IP addresses may follow **set ip default next-hop**.

If weight follows **ip address**, up to 4 nexthop addresses can be configured.

Note: 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, if the **weight** of a **nexthop** address is configured, it is 1 by default.

Differences between **set ip next-hop** and **set ip default next-hop**: After **set ip next-hop** is configured, the routing policy takes precedence over the routing table; while after **set ip default next-hop** is configured, the routing table takes precedence over the routing policy.

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 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, which are usually in this order:

- **set ip next-hop**
- **set interface**
- **set ip default next-hop**
- **set default interface**

Examples

The following example forwards the packets from two different nodes to different routes.

For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding routes, 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 routes, they are forwarded to device 7.7.7.7. The other messages will be discarded if the software cannot find the forwarding routes.

```
!
access-list 1 permit ip 1.1.1.1 0.0.0.0
access-list 2 permit ip 2.2.2.2 0.0.0.0
```

```
!
interface async 1
ip policy route-map equal-access
!
route-map equal-access permit 10
match ip address 1
set ip default next-hop 6.6.6.6
route-map equal-access permit 20
match ip address 2
set ip default next-hop 7.7.7.7
route-map equal-access permit 30
set default interface null0
```

Related commands

Command	Description
route-map	Define the route map
match ip address	Match the address in the access list
set default interface	Set the default packet output interface.
set default interface	Set the default packet output interface.
set interface	Set the packet output interface
set ip next-hop	Set the default next hop of the packets.
set ip precedence	Set the priority of the packets.

31.1.29 set ip tos

To set the TOS of the transmitted message IP header that matches the route map match rule, use the route map configuration command **set ip tos**. The **no** form of this command is used to delete the existing configuration of the TOS value.

set ip tos {*<0-15>* | *max-reliability* | *max-throughput* | *min-delay*

| *min-monetary-cost* | *normal* }

no set ip tos {*<0-15>* | *max-reliability* | *max-throughput* | *min-delay*

| *min-monetary-cost* | *normal* }

Default configuration Not configured.

Command mode Route map configuration mode.

Usage guidelines

Setting the TOS value in the IP message header frequently enables the policy-based routing to transmit the routed IP messages at different quality of service.

In the route map configuration rule, it is possible to configure multiple **set ip tos** commands but only the last one takes effect. The IP header of all matched messages by the policy-based routing will have specified TOS configured.

Examples

In the example below, the TOS is set as 4 for the messages that come from fastEthernet 0/0 and have source address 192.168.217.68.

```
access-list 1 permit 192.168.217.68
route-map name
match ip address 1
set ip tos 4
int f 0/0
ip policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface of the route.
match ip address	Match the address in the access list.
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 route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.
set ip precedence	Set the precedence field in the IP header

31.1.30 set ip precedence

To set the precedence of the transmitted message IP header that matches the route map match rule, use the route map configuration command **set ip precedence**. The **no** form of this command is used to delete the existing configuration of the precedence value.

set ip precedence {<*0-7*> | *critical* | *flash* | *flash-override* |

immediate | *internet* | *network* | *priority* | *routine* }

no set ip precedence {*<0-7>* | *critical* | *flash* | *flash-override*

immediate | *internet* | *network* | *priority* | *routine* }

Default configuration	No default configuration.
Command mode	Route map configuration mode.
Usage guidelines	Setting the precedence value in the IP message header frequently enables the policy-based routing to transmit the routed IP messages at different priorities. In the route map configuration rule, it is possible to configure multiple **set ip precedence** commands but only the last one takes effect. The IP header of all matched messages by the policy-based routing will have specified precedence configured.

Examples	In the example below, the precedence is set as 4 for the messages that come from fastEthernet 0/0 and have source address 192.168.217.68.
	`access-list 1 permit 192.168.217.68`
	`oute-map-name`
	`match ip address 1`
	`set ip precedence 4`
	`int f 0/0`
	`ip policy route-map name`

Related commands

Command	Description
match interface	Match the next-hop interface of the route.
match ip address	Match the address in the access list.
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 route metric.
match route-type	Match the route type.
match tag	Match the route tag.

set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.
set ip tos	Set the tos in the IP header

31.1.31 set default interface

To specify the default forwarding interface for the packets without clear routes, run the route map configuration command **set default interface**. Use the **no** form of this command to delete the setting.

set default interface *interface-type interface-number* [*…interface-type interface-number*]

no set default interface *interface-type interface-number*

[*…interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.

Default

No default configuration.

Command mode

Route map configuration mode

Usage guidelines

Multiple interfaces may follow **match interface**.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the router will determine how to process the packets to be routed according to the route map, which determines the next-hop router 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.

If the first defined interface becomes "down", the interface set by the second **set** command will be attempted.

A route-map policy may contain multiple **set** operations, which are

usually in this order:

- **set ip next-hop**
- **set interface**
- **set ip default next-hop**
- **set default interface**

If the interface is set as null 0, the packets will be discarded.

Examples

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic with packet size smaller than 500 bytes on the interface, without clear routes in the routing table, through fastethernet 1/0 interface.

```
interface serial 1/0
ip policy route-map smallpak

route-map smallpak permit 10
match length 0 500
set default interface fastethernet 1/0
```

Related commands

Command	Description
route-map	Set the route map.
match ip address	Match the address in the access list.
match length	Match packet size range
set interface	Set the packet output interface
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets
set ip precedence	Set the priority of the packets.

31.1.32 set interface

To specify the forwarding interface for the packets to match the rules, run the route map configuration command **set interface**. Use the **no** form of this command to delete the setting.

set interface *interface-type interface-number* [*…interface-type interface-number*]

no set interface *interface-type interface-number* [*…interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Interface type.
interface-number	Interface ID

Default	No default configuration.
Command mode	Route map configuration mode
Usage guidelines	Multiple interfaces may follow **match interface**. Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the router will determine how to process the packets to be routed according to the route map, which determines the next-hop router 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. If the first defined interface becomes "down", the interface set by the second **set** command will be attempted. A route-map policy may contain multiple **set** operations, which are usually in this order: ■ **set ip next-hop** ■ **set interface** ■ **set ip default next-hop** ■ **set default interface** If the interface is set as null 0, the packets will be discarded.

Examples	In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic with packet size smaller than 500 bytes on the interface through fastethernet 0/0 interface.
	`interface serial 1/0`
	`ip policy route-map smallpak`
	
	`route-map smallpak permit 10`
	`match length 0 500`
	`set interface fastethernet 0/0`

Related commands

Command	Description
route-map	Set the route map.
match ip address	Match the address in the access list.
match length	Match packet size range
set default interface	Set the default packet output interface.
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets
set ip precedence	Set the priority of the packets.

31.1.33 ip prefix-list

Use this command to create a prefix list or add an entry in the prefix list. Use the **no** form of this command to delete an entry in the prefix list.

ip prefix-list *prefix-lis-name*[**seq** *seq-number*] { **deny** | **permit**}

ip-prefix [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

no ip prefix-list *prefix-lis-name*[**seq** *seq-number*] { **deny** | **permit**}

ip-prefix [**ge** *minimum-prefix- length*][**le** *maximum-prefix- length*]

Parameter description

Parameter	Description
prefix-lis-name	Name of the prefix list.
seq-number	Sequence number of an entry in the prefix list. Its range is 1~4294967294. 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	(Optional) Allow the access to the matching result.
deny	(Optional) Deny the access to the matching result.
ip-prefix	Set the network address and its mask. The network address can be any valid IP address. The mask can be 0~32 characters.
minimum-prefix-length	(Optional) Specify the minimum range (that is,

	the start length of the range). Note: **ge** indicates the "≥" operation.
maximum-prefix-length	(Optional) Specify the maximum range (that is, the end length of the range). Note: **le** indicates the "≤" operation.

Default configuration

No prefix list is created.

Command mode

Global configuration mode

Usage guidelines

ip prefix-list is used configure the IP prefix filter. The prefix list decides the action according to the "permit" or "deny" keyword.

The prefix list is used to set exact match or fuzzy match of a prefix. **ge** or **le** is used to set the prefix match range, which is more flexible than ip-prefix. If neither **ge** nor **le** is used, ip-prefix provides the exact match range. If only **ge** is used, the match range is from minimum-prefix-length to 32. If only **le** is used, the match range is from ip-prefix mask length to maximum-prefix- length. If both **ge** and **le** are used, the match range is from minimum-prefix-length to maximum-prefix- length. That is to say, the relationships between ip-prefix mask, minimum-prefix-length and maximum-prefix-length are as follows:

ip-prefix mask length < minimum-prefix-length < maximum-prefix-length <= *32*

Examples

The example below shows how to filter by using the distribute list. For example, if you want to filter the route distribution information outputted in the OSPF during redistribution to the RIP according to the destination IP address, you can define the filtering rule in the associated IP prefix list (for example, only allowing the routing information whose destination IP address is 201.1.1.0/24 to be distributed) by performing the following steps:

```
DGS-3610# configure terminal
DGS-3610(config)# ip prefix-list pre1 permit 201.1.1.0/24
DGS-3610(config)# router ospf
DGS-3610(config-router)# distribute-list prefix pre1 out rip
Switch(config-if)#end
```

31.1.34 ip ref ecmp load-balance source

If the ECMP/WCMP route exists in the hardware forwarding table in the switch, load-balance policies also exist. When the route has multiple next hops, the hardware can select a next hop according to the policy set.

This policy can be expressed as HASH(KEY(SIP,[DIP] [TCP/UDP Port] [UDF])).

This expression is interpreted as it will carry out the Hash operation by a keyword, and adopt the operated value to select the next hop. Where, the strategy that can be set includes two aspects, the one is the selection of the HASH algorithm. The hardware can provide two selections such as CRC32_Upper and CRC32_Lower. The other one is KEY, which can be formed by selecting some fields of the packet. By default, it only selects the source IP address (SIP). At the same time, it can add to select the value of the corresponding port for the TCP/UDP packet, the destination IP of the packet (DIP) and the user-defined value, so as to form the KEY.

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]}

Command mode	Global configuration mode.
Usage Guidelines	Use any combination of DIP, Port and UDF for the generation of the Key. And select CRC32_Lower or CRC32_Upper as a Hash algorithm. The no command will remove the keyword carried as part of the Key based on the system stored setting. For example, the system stored settings are SIP + DIP + Port. After the no ip ref ecmp route dip port command is executed, the component of the Key is only the SIP. If the member following the no command is not in the system stored setting, the execution of this command will not experience an error.

Examples	Configure the hardware load-balance hash algorithm
	`DGS-3610(config)# ip ref ecmp load-balance crc32_upper`
	Configure the hardware load-balance algorithm keyword as the source ip (by default), destination ip and udp/tc port.
	`DGS-3610(config)# ip ref ecmp load-balance dip port`

Related commands

Command	Description
None	

31.2 Showing Related Command

31.2.1 show route-map

Use this command to view the configuration of the route map.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
route-map-name	(Optional) Specify 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

```
DGS-3610# 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. Decides whether to perform the **set** operation according to the "permit" or "deny" keyword in the route map.
Set clauses	Set the operation after the rule matches.

31.2.2 show ip prefix-list

Use this command to view the prefix list or the entries in it.

show ip prefix-list [*prefix-name*

Parameter description

Parameter	Description
prefix-name	Name of the prefix list.
seq-num	(Optional) The sequence number of the specified entry in the prefix list.
ip-prefix	(Optional) The specified network prefix.

Default configuration

The configuration information of all the prefix lists is 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

```
DGS-3610# 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
```

31.2.3 show ip ref

This command is used to display the current global statistics of REF, including the number of existing routes, number of adjacent nodes, number of load balancing tables, and number of weight nodes.

Command mode

Privileged user mode.

Usage guidelines

This command can be used to show the route storage information and statistics of each architecture in REF.

Examples

```
DGS-3610# show ip ref
-----------statistic information-----------:
current    routes: 5
alloc weight_nodes: 5
alloc  bal_tables: 0
alloc   adj_nodes: 5
alloc     res_adj: 0
----------------------------------------:
```

The fields in the displayed results are described as follows:

Field	Description
routes	Number of routes in the REF table
weight_nodes	Number of weight nodes
bal_tables	Number of load balancing tables
adj_nodes	Number of adjacent nodes
res_adj	Number of registration and resolution nodes

Parameter description

32 Configuring PBR Command

32.1 Configuration Related Commands

32.1.1 ip policy route-map

To enable the policy-based routing on an interface, run the interface configuration command **ip policy route-map**. The **no** form of this command disables the application of policy-based routing.

ip policy route-map *route-map*

no ip policy route-map *route-map*

Parameter description

Parameter	Description
route-map	Name of the route map

Default

Disabled the policy-based routing by default.

Command mode

Interface configuration mode.

Usage guidelines

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the router will determine how to process the packets to be routed according to the route map, which determines the next-hop router of the packets.

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.

Examples

In the example below, when the fast Ethernet interface FE0 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, it forwards it normally.

```
access-list 1 permit 10.0.0.1
access-list 2 permit 20.0.0.1
route-map lab1 permit 10
match ip address 1
set ip next-hop 196.168.4.6
exit
route-map lab1 permit 20
match ip address 2
set ip next-hop 196.168.5.6
exit
interface FastEthernet 0/0
ip policy route-map lab1
exit
```

Related commands

Command	Description
access-list	Set the access list.
route-map	Set the route map.

32.1.2 ip local policy route-map

To enable the policy-based routing for messages sent locally, run the interface configuration command **ip local policy route-map**. The **no** form of this command disables the application of policy-based routing.

ip local policy route-map *route-map*

no ip local policy route-map *route-map*

Parameter description

Parameter	Description
route-map	Name of the route map.

Default

The policy routing is disabled by default.

Command mode

Configuration mode.

Usage guidelines	Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the router will determine how to process the packets to be routed according to the route map, which determines the next-hop router of the packets. 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.

Examples	In the example below, the messages from the source address 192.168.217.10 on the local machine are sent out from f0/0.
	`access-list 1 permit 192.168.217.10`
	`route-map lab1 permit 10`
	`match ip address 1`
	`set interface f 0/0`
	`exit`

Related commands

Command	Description
access-list	Set the access list.
route-map	Define the route map.

32.1.3 ip policy

To set the "**set nexthop**" of the policy-based routing to work in the redundant backup or load balancing mode, run the "**ip policy**" in the global configuration mode.

ip policy [**load-balance|redundance**]

Caution NPE80 does not support this command.

Parameter description

Parameter	Description
[**load-balance	redundance**]	Specify the load balancing or redundant backup mode.

Default

Redundant backup.

Command mode

Global configuration mode.

Usage guidelines

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the router will determine how to process the packets to be routed according to the route map, which determines the next-hop router of the packets.

In configuring the "**set next-hop**" in the sub-route map, it is possible to configure multiple next hops. However, when configuring redundant backup, the only the first one of the policy routes can be parsed as the next-hop function. When the load balancing is set, multiple policy routes can be parsed as the function of next hop. The WCMP can be set with four next hops, and the ECMP can be set with up to 32 next hops.

Examples

In the example below, there are multiple next hops configured in the route map. When the redundant backup is set in the global configuration mode, only the first next hop among the sub-route map of the policy routes applied on the EF0 takes effect and performs forwarding.

```
access-list 1 permit 10.0.0.1
access-list 2 permit 20.0.0.1
route-map lab1 permit 10
match ip address 1
set ip next-hop 196.168.4.6
set ip next-hop 196.168.4.7
set ip next-hop 196.168.4.8
exit
route-map lab1 permit 20
match ip address 2
set ip next-hop 196.168.5.6
set ip next-hop 196.168.5.7
set ip next-hop 196.168.5.8
exit
interface FastEthernet 0/0
ip policy route-map lab1
exit
ip policy redundance
```

Related commands

Command	Description
set ip next-hop	Define the next hop of policy-based routing
set ip default next-hop	Define the default next hop of policy-based routing
set interface	Define the exit of policy-based routing
set default interface	Define the default exit of policy-based routing
set tos	Set the tos in the message IP header
set preference	Set the priority in the message IP header
match ip address	Set the filtering rule.
match length	Match message length
route-map	Define the route map.

Caution

The relevant command of route-map configuration, please refer to the *Protocol-independent Command Reference*.

33 Configuring IPv6 Commands

33.1 Configuration Related Commands

The IPv6 configuration commands include:

- **ping ipv6**
- **ipv6 address**
- **ipv6 enable**
- **ipv6 neighbor**
- **ipv6 route**
- **ipv6 ns-linklocal-src**
- **ipv6 nd ns-interval**
- **ipv6 nd reachable-time**
- **ipv6 nd prefix**
- **ipv6 nd ra-lifetime**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-hoplimit**
- **ipv6 nd ra-mtu**
- **ipv6 nd managed-config-flag**
- **ipv6 nd other-config-flag**
- **ipv6 nd dad attempts**
- **ipv6 nd suppress-ra**
- **ipv6 redirects**
- **show ipv6 route**
- **show ipv6 neighbors**
- **show ipv6 interface**
- **clear ipv6 neighbors**
- **tunnel destination**
- **tunnel mode ipv6ip**
- **tunnel source**

- **tunnel ttl**

33.1.1 ping ipv6

Use this command to check the connectivity of the IPv6 network.

ping ipv6 [*ipv6-address*]

Parameter description

Parameter	Description
ipv6-address	Diagnosed destination address

Command mode

Privileged mode.

Usage guidelines

If no user address is entered, the user interaction mode is entered, and you can specify the parameters. Description of the symbols returned:

Signs	Meaning
!	The response to each request sent is received.
.	The response to the request sent is not received.
U	Indicate the device has no route reaching the destination host
R	Parameter error.
F	No system resource is available.
A	The source address of the packet is not selected.
D	The network interface is Down, or the IPv6 function of the interface is disabled (for example, address collision is detected).
?	Unknown error

Examples

```
DGS-3610# ping ipv6 fec0::1
```

33.1.2 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to delete the setting.

ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]

no ipv6 address [*ipv6-prefix/prefix-length*] [**eui-64**]

Parameter

Parameter	Description

description	*ipv6-prefix*	IPv6 address, which shall be in the format defined in RFC2373. 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, namely the length of the network ID in the IPv6 address.  **Caution** Because the range of route prefix length supported by the hardware transmit table of DGS-3610 series switches is [0, 64] or [128, 128], the prefix length range of the IPv6 address interface is [0, 64] or [128, 128].
	eui-64	Means that the generated ipv6 addresses consists of the address prefix and the 64-bit interface ID

Command mode	Interface configuration mode
Usage guidelines	If **eui-64** is used, the length of the prefix shall be 64. When an IPv6 interface is created and the link state is Up, the system will automatically generates local address for the interface. If no address is specified in **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**.

Examples	`DGS-3610(config-if)# ipv6 address 2001:1::1/64`
	`DGS-3610(config-if)# no ipv6 address 2001:1::1/64`
	`DGS-3610(config-if)# ipv6 address 2002:1::1/64 eui-64`
	`DGS-3610(config-if)# no ipv6 address 2002:1::1/64 eui-64`

33.1.3 ipv6 enable

Use this command to enable the IPv6 function of 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 using **ipv6 enable** or by configuring IPv6 address for the interface. Note: If an IPv6 address is configured for the interface, the IPv6 function of the interface will be enabled automatically and cannot be disabled with **no ipv6 enable**.
Examples	DGS-3610(config-if)# **ipv6 enable**

Related commands

Command	Description
show ipv6 interface	Show the interface information.

33.1.4 ipv6 hop-limit

In the global configuration mode, this command is used to configure the default hops to send unicast messages.

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	DGS-3610(config)# **ipv6 hop-limit** *100*

33.1.5 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to delete 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 shall be in the format defined in RFC2373.
interface-id	Specify the network interface of the neighbor (Routed Port, L3 AP interface, or SVI interface).
hardware-address	Link 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, this command can only configure a static neighbor for an IPv6 interface.

If the neighbor to be configured has been learnt through NDP and has been stored in the neighbor list, the dynamically generated neighbor will be automatically switched to a static one. A static neighbor is always in the Reachable state.

Use **clear ipv6 neighbors** to clear all the neighbors dynamically learnt through NDP.

Use **show ipv6 neighbors** to view the neighbor information.

Examples

```
DGS-3610(conifg)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related commands

Command	Description
show ipv6 interface	Show the neighbor information.
clear ipv6 neighbors	Clear the dynamically learnt neighbors.

33.1.6 ipv6 source-route

This command is used to make the router forward the IPv6 packet with the first route part, and the no form of this command is used to prohibit the router forward the IPv6 packet with the first route part.

ipv6 source-route

no ipv6 source-route

Parameter description	None
Default configuration	Prohibit to forward the IPv6 packet with the first route part.
Command mode	Global configuration mode.
Usage guidelines	For the first route part of the type o presents the security hazard, it makes the router easy to suffer from the DoS attack. Hence, by default, it prohibits to forward the IPv6 packet with the first route part. However, it still processes the IPv6 packet whose final destination address is the first route part of the type o for this equipment.
Examples	`DGS-3610(conifg)# no ipv6 source-route`

Related commands

Command	Description
None	

33.1.7 ipv6 route

Use this command to configure an IPv6 static route. Use the **no** form of this command to delete the setting.

ipv6 route *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-id* [*ipv6-address*]}

no ipv6 route *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-id* [*ipv6-address*]}

Parameter description

Parameter	Description
ipv6-prefix	IPV6 network number, compliant with the RFC2373 address denotation format prefix-length.Length of the IPv6 prefix. "/" shall proceed it.  **Caution** Because the range of route prefix length supported by the hardware transmit table of DGS-3610 series switches is [0, 64] or [128, 128], the prefix length range of the IPv6 address interface is [0, 64] or [128, 128].
ipv6-address	Specify the next-hop address toward the destination address. It shall be in the format defined in RFC2373. The next-hop address and the next-hop interface can be specified at the same time. Note that if the next-hop address is a link-local address, the output interface shall be specified.
interface-id	Specify the packet output interface toward the destination network. If the static route is configured with output interface but not next-hop address, the destination will be considered to be on the link connected with the output interface; that is to say, the static route will be treated as a direct route. Note that if the destination network or next-hop address is a link-local address, the output interface shall be specified.

Command mode

Global configuration mode.

Usage guidelines

If the destination address or next-hop address is a link-local address, the output interface shall be specified; if the destination address is a link-local address, the next-hop shall be also a link-local address. In configuring a route, the destination address and the next-hop address shall not be multicast address. If both the next hop and the output interface are specified, the output interface of the direct route that matches the next hop shall be the same as the configured output interface.

Examples

```
DGS-3610(config)# ipv6 route 2001::/64 vlan 1 2005::1
```

Related commands

Command	Description
show ipv6 route	Show the IPv6 route information.

33.1.8 ipv6 ns-linklocal-src

When this command is executed, the local address of the link will be used as the source address in sending neighbor request. When “no ipv6 ns-linklocal-src“ is executed, the global address will be used as the source address in sending neighbor request.

ipv6 ns-linklocal-src

no ipv6 ns-linklocal-src

Default configuration The local address of the link is always used as the source address in sending neighbor request.

Command mode Global configuration mode.

Usage guidelines Omitted

Examples

```
DGS-3610(config)# no ipv6 ns-linklocal-src
```

33.1.9 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 the default setting.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Parameter description

Parameter	Description
milliseconds	Interval for retransmitting NS, measured in milliseconds. The range is 1000-3600000. 1000-3600000

Default configuration The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000ms(1s).

Command Interface configuration mode.

mode

Usage guidelines

The configured value will be advertised through RA and will be used by the router itself. It is not recommended to set a too small interval.

Examples

```
DGS-3610(conifg-if)# ipv6 nd ns-interval 2000
```

Related commands

Command	Description
show ipv6 interface	Show the interface information**.**

33.1.10 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learnt through NDP. Use the **no** form of this command to restore the default setting.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Parameter description

Parameter	Description
milliseconds	Time to consider neighbor reachable, in milliseconds, range: 0-3600000

Default configuration

The default value in RA is 0 (unspecified); the reachable time is 30000ms(30s).

Command mode

Interface configuration mode.

Usage guidelines

The router uses the time set here to check the unreachable neighbor. A smaller time means that the router can check the neighbor failure more quickly, but more network bandwidth and device resource will be used. Therefore, it is not recommended to set a too small reachable time.

The configured value will be advertised through RA and will be used by the router itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.

Examples

```
DGS-3610(conifg-if)# ipv6 nd reachable-time 1000000
```

	Command	Description
Related commands	**show ipv6 interface**	Show the interface information.

33.1.11 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 setting or restore the default setting.

ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **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. It shall be in the format defined in RFC2373.
prefix-length	Length of the IPv6 prefix. “/” shall proceed it.
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 end time of the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
infinite	Always valid.
default	Set the default parameters.
no-advertise	The prefix will not be advertised by the router.
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	This option indicates 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 guidelines	This command can be used to configure the parameters of 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** Sets 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.
	`DGS-3610(conifg)# interface vlan 1`
	`DGS-3610(conifg-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):`
	`DGS-3610(conifg)# interface vlan 1`
	`DGS-3610(conifg-if)# ipv6 nd default no-autoconfig`
	If no parameter is specified for an added, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related commands

Command	Description
show ipv6 interface	Show ra-info of an interface.

33.1.12 ipv6 nd ra-lifetime

Use this command to set the “router lifetime” in the RA sent by the interface. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameter description

Parameter	Description
seconds	This device is used as the default valid time of the device on the interface

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 host on the link of the interface can select the router as the default router. If the value is set to 0, the router will not serve as the default router any longer. If it is not set to 0, it shall be larger than or equal to ra-interval.

Examples

```
DGS-3610(conifgf)# interface vlan 1
DGS-3610(conifg-if)# ipv6 nd ra-lifetime 2000
```

Related commands

Command	Description
show ipv6 interface	Show ra-info of an interface.
ipv6 nd ra-interval	Set the interval for sending RA.

33.1.13 ipv6 nd ra-interval

Use this command to set the interval for the interface to send RA. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-interval *seconds*

no ipv6 nd ra-interval

Parameter description

Parameter	Description
seconds	Router advertisement (RA) message sent interval, in seconds

Default configuration

200s

Command mode

Interface configuration mode.

Usage guidelines

If the router serves as the default router, the interval set here shall not be larger than the lifetime of the router. Besides, to ensure other routers along the link occupies network bandwidth while sending RA, the actual interval for sending RA is 20% more or less than the value set here.

Examples

```
DGS-3610(conifgf)# interface vlan 1
DGS-3610(conifg-if)# ipv6 nd ra-interval 110
```

Related commands

Command	Description
show ipv6 interface	Show ra-info of an interface.
ipv6 nd ra-lifetime	Set the alive period of the device

33.1.14 ipv6 nd ra-hoplimit

Use this command to set the interval for the interface to send RA. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-hoplimit *value*

no ipv6 nd ra-hoplimit

Parameter description

Parameter	Description
value	Value of the router advertisement (RA) message hop field

Default configuration

The default value is 64

Command mode	Interface configuration mode.
Usage guidelines	It is used to set the value of the router advertisement message hop field
Examples	`DGS-3610(config)# interface vlan 1` `DGS-3610(config -if)# ipv6 nd ra-hoplimit 110`

Related commands

Command	Description
show ipv6 interface	Show **ra-info** of an interface.
ipv6 nd ra-lifetime	Set the alive period of the device
ipv6 nd ra-interval	Set the interval for sending RA.
ipv6 nd ra-mtu	Set the value of the router advertisement (RA) message MTU field

33.1.15 ipv6 nd ra-mtu

Use this command to set the interval for the interface to send RA. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-mtu *value*

no ipv6 nd ra-mtu

Parameter description

Parameter	Description
value	Value of the router advertisement (RA) message MTU field

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

```
DGS-3610(config)# interface vlan 1
DGS-3610(config -if)# ipv6 nd ra-mtu 1400
```

Related commands

Command	Description
show ipv6 interface	Show ra-info of an interface.
ipv6 nd ra-lifetime	Set the alive period of the device
ipv6 nd ra-interval	Set the interval for sending RA.
ipv6 nd ra-hoplimit	Set the value of the router advertisement (RA) message hops field

33.1.16 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag in the RA. Use the **no** form of this command to clear the setting.

ipv6 nd managed-config-flag

no ipv6 managed-config-flag

Default configuration

Not configured.

Command mode

Interface configuration mode.

Usage guidelines

This flag determines whether the host that receives the RA obtains address through stateful auto configuration. If the flag is set, the host obtains address through stateful auto configuration, otherwise it does not.

Examples

```
DGS-3610(config)# int vlan 1
DGS-3610(config)# ipv6 nd managed-config-flag
```

Related commands

Command	Description
show ipv6 interface	Show **ra-info** of an interface.
ipv6 nd other-config-flag	Set the flag for obtaining all information except address through stateful auto configuration.

33.1.17 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 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 of the interface is disabled. The range is 0-600

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” state. 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

```
DGS-3610(conifgf)# interface vlan 1
DGS-3610(conifg-if)# ipv6 nd dad attempts 3
```

Related commands

Command	Description
show ipv6 interface	View the interface information.

33.1.18 ipv6 nd suppress-ra

Use this command to disable the interface from sending RA. Use the **no** form of this command to enable the function.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	Use this command to disable an interface from sending RA.
Examples	`DGS-3610(conifgf)# interface vlan 1` `DGS-3610(config-if)# ipv6 suppress-ra`

Related commands

Command	Description
show ipv6 interface	Show **ra-info** of an interface.

33.1.19 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	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	The transmission rate of any ICMPv6 error packets is limited. By default, it is 100pps.

Examples

```
DGS-3610(conifgf)# interface vlan 1
DGS-3610(config-if)# ipv6 redirects
```

Related commands

Command	Description
show ipv6 interface	Show the interface information.

33.1.20 clear ipv6 neighbors

Use this command to clear the dynamically learnt neighbors.

clrear ipv6 neighbors

Command mode

Privileged mode.

Usage guidelines

This command can be used to clear all the neighbors dynamically learnt by the RDP. Note that the static neighbors will not be cleared.

Examples

```
DGS-3610# clear ipv6 neighbors
```

Related commands

Command	Description
ipv6 neighbor	Configure table neighbor
show ipv6 neighbors	Show the neighbors.

33.1.21 tunnel mode ipv6ip

Use this command to configure static IPv6 tunnel mode. Use the **no** form of this command to restore the default IPv6 tunnel mode.

tunnel mode ipv6ip [**6to4 | isatap**]

no tunnel mode

Parameter description

Parameter	Description
6to4	Configure the tunnel as the 6to4 auto tunnel
isatap	Configure the tunnel as an ISATAP auto tunnel.

Default configuration

The type of an configured IPv6 tunnel is a manual tunnel.

Command mode

Interface configuration mode.

Usage guidelines

After a tunnel interface 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 need be specified.

Examples

The following example configures a 6to4 tunnel.

```
DGS-3610(config)# interface tunnel 1
DGS-3610(config-if)# tunnel mode ipv6ip 6to4
DGS-3610(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.·

33.1.22 tunnel destination

Use this command to specify the destination address for the tunnel interface. Use the **no** form of this command to delete the setting.

tunnel destination *ipv4-address*

no tunnel destination

Parameter description

Parameter	Description
ipv4-address	Destination address of the tunnel.

Default configuration

Not configured.

Command mode

Interface configuration mode.

Usage guidelines

A router shall not be configured multiple tunnels with the same encryption type, source address and destination address.

Note: For auto tunnel (6to4 and isatap), the destination address shall not be configured.

Examples

The following example configures an IPv6 manual tunnel.

```
DGS-3610(config)# interface tunnel 1
DGS-3610(config-if)# tunnel mode ipv6ip
DGS-3610(config-if)# tunnel source vlan 1
DGS-3610(config-if)# tunnel destination 192.168.5.1
```

Related commands

Command	Description
tunnel source	Configure the source address of the tunnel.
tunnel mode	Configure the mode of a tunnel.

33.1.23 tunnel source

Use this command to specify the source address for the tunnel interface. Use the **no** form of this command to delete the setting.

tunnel source {*ipv4-address* | *interface-type interface-number*}

no tunnel source

Parameter description

Parameter	Description
ipv4-address	Configure the source IPv4 address of the tunnel, which will be used as the source address in the packet to be transmitted in the tunnel.
interface-type interface-number	Configure the interface used by the tunnel source, which will be used as the source IPv4 address in the packet to be transmitted in the tunnel.

Default configuration

Not configured.

Command mode

Interface configuration mode.

Usage guidelines

The source address of a tunnel can be a specified IPv4 address or an IPv4 address of an interface. In configuring an auto tunnel (for example, 6to4 and isatap), it is recommended to specify the source address.

A router shall not be configured multiple tunnels with the same encryption type, source address and destination address.

If there are multiple auto tunnels, their source addresses shall be different.

Examples

The following example configures an IPv6 manual tunnel.

```
DGS-3610(config)# interface tunnel 1
DGS-3610(config-if)# tunnel mode ipv6ip
DGS-3610(config-if)# tunnel source vlan 1
DGS-3610(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.·

33.1.24 tunnel ttl

This command is used to specify the TTL value of the IPv4 part in the encapsulated IPv6 messages. The **no** command of it restores the default 128.

tunnel ttl *value*

no tunnel ttl

Parameter description

Parameter	Description
value	TTL value

Default configuration

The default value is 128

Command mode

Interface configuration mode.

Usage guidelines

This command is used to specify the TTL value of the IPv4 part in the encapsulated IPv6 messages.

Examples

```
DGS-3610(config)# interface tunnel 1
DGS-3610(config-if)# tunnel ttl 64
```

Related commands

Command	Description
tunnel mode	Configure the mode of a tunnel.
tunnel source	Configure the source address of the tunnel.
tunnel destination	Configure the destination address of a tunnel.·

33.2 Showing Related Command

33.2.1 show ipv6 route

Use this command to show the IPv6 route information.

show ipv6 route [**static**] [**local**] [**connected**]

Parameter description

Parameter	Description
static	Show static route configuration
local	Show the local route.
connected	Show directly-connected route

Command mode

Privileged mode.

Usage guidelines

Use this command to view the routing table.

Examples

```
DGS-3610# 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

Command	Description

commands	**ipv6 route**	Configure static routes

33.2.2 show ipv6 neighbors

Use this command to show the IPv6 neighbors.

show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]

Parameter description

Parameter	Description
verbose	Show the neighbor details.
interface-id	Show the neighbors of the specified interface.
ipv6-addres	Show the information of the specified neighbor

Command mode

Privileged mode.

Usage guidelines

Show the neighbors of SVI 1:

```
DGS-3610# 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:
DGS-3610# 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	Neighbor IPv6 address
Linklayer Addr	Link address, namely, Mac address. If it is not available, “incomplete” is displayed.
Interface	Interface of the neighbor.
State	State of the neighbor: state/H(R) The values of STATE include: 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

```
DGS-3610# show ipv6 neighbors
```

Related commands

Command	Description
ipv6 neighbor	Configure table neighbor

33.2.3 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 view the address configuration, ND configuration and other information of an IPv6 interface.

Examples

```
DGS-3610# 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
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 router 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 [] behind the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	It indicates that the address is an anycast address.

TENTATIVE	It indicates that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	It indicates that a duplicate address exists.
DEPRECATED	It indicates that the preferred lifetime of the address expires.
NODAD	It indicates that no DAD is implemented for the address.
AUTOIFID	It indicates that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.

```
DGS-3610# 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 router advertisements live for 1800 seconds
ND router 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)	It indicates whether the RA timer is started.
waits	It indicates that the RS is received but the number of the responses is not available.
initcount	It indicates the number of the RAs when the RA timer is restarted.

RA(out/in/ inconsistent)	out: It indicates the number of the RAs that are sent. In: It indicates the number of the RAs that are received. inconsistent: It indicates the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the router.
RS(input)	It indicates 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 in Prefix of ra-info:

Field	**Meaning**
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	It indicates that the interfaces use the default prefix.
Auto | CFG	Auto: It indicates the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: It indicates that the prefix is manually configured.
!Adv	It indicates 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: It indicates that the on-link in the prefix is set. !L:It indicates that the on-link in the prefix is not set.
A | !A	A: It indicates that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

34 Configuring IPv6 Routing Protocol Commands

34.1 Configuration Related Commands

34.1.1 area default-cost

Set this command for the ABR in the stub or NSSA area. It's used for defining the default routing cost within the stub or NSSA area. Use the **no** form of this command to restore the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter description

Parameter	Description
area-id	The area ID of the stub or NSSA area. It can be an integer or an prefix of IPv4 .
cost	Default routing cost of the stub or NSSA area. Its range is 1~16777214.

Default configuration

By default, **default-cost** is 1.

Command mode

OSPFv3 configuration mode.

Usage guidelines

This command can only work in the ABR of the stub or nssa area.

Examples

The following example sets the default routing cost of stub area 50 to 100.

```
ipv6 router ospf 1
area 50 stub
area 50 default-cost 100
```

Related commands

Command	Description
area stub	Sets a stub area.
show ipv6 ospf area	Shows the OSPFv3 area information.

34.1.2 area-range

Use this command to set the range of the summarized inter-area addresses. Use the **no** form of this command to delete the configured t range of the summarized or restore the default parameters within the range of the summarized.

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 summarized. It can be an integer or an IPv4 prefix.
ipv6-prefix/prefix-length	Range of the summarized addresses.
not-advertise	The range of the summarized addresses is not advertised. By default, the function is enabled.

Default configuration

No summarized inter-area address range is defined.

Command mode

OSPFv3 configuration mode.

Usage guidelines

This command applies only to ABR. Use this command to summarize multiple routes in 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 this area including all the configuration in this area.

Examples

The following example summarizes the routes in area 1.

```
ipv6 router ospf 1
area 1 range 2001:abcd:1:2::/64
```

Related commands

Command	Description
discard-route	Sets whether to add the discard route generated by the OSPF process to the core routing table.
summary-prefix	Sets the summarized address range of the external route.
show ipv6 ospf area-range	Shows the summarized inter-area address range in the OPFv3 area.

34.1.3 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	The area ID of the stub or NSSA area. 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 LSA with type 3 default route to the stub area and does not advertise other type 3 LSAs.

Default configuration

Undefined the Stub area.

Command mode

OSPFv3 configuration mode.

Usage guidelines

Use **no area** *area-id* **stub** command to restore the area as a normal area.

Use **no area** *area-id* to delete the area including the all configuration in the area.

By default, the ABR in the stub area only generates and then advertises the LSA with type 3 default route to the stub. While the ABR in the NSSA area stub generates and then advertises the LSA with type 3 default 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	Sets the cost of the default route in the stub or NSSA area.
	show ipv6 ospf area	Shows the OSPFv3 area information.

34.1.4 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 its default setting.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

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*	The interval of the hello packet sent from local virtual link interface. The range is from 1 to 65535s, the default value is 10s.
	dead-interval *seconds*	The failed interval of the neighbor is taken when it is on the local interface of the virtual link . Its range is 1-65535s, and the default value is four times the value of **hello-interval**.
	retransmit-interval *seconds*	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 *seconds*	Delay for the local interface of the virtual link to send LSA. The range is from 1 to 65535s, the default value is 1s.

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 routing information in the whole OSPF AS. If an area cannot be directly connected with the backbone area, it can be connected with the latter through a virtual link. Cautions: ■ The virtual link shall be not in the stub or NSSA area. ■ **hello-interval**, **dead-interval** and **instance** should be configured consistently on both sides of the virtual link, otherwise neighboring relationship cannot be created between the virtual neighbors. ■ Use **no area** *area-id* to delete the area including the all configuration in 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	Shows the OSPFv3 routing process information.
show ipv6 ospf neighbor	Shows the OSPFv3 neighbor information.
show ipv6 ospf virtual-links	Shows the OSPFv3 virtual link information.

34.1.5 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 the default reference bandwidth.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter description

Parameter	Description
reference-bandwidth *ref-bw*	Reference bandwidth, measured in Mbps. Its range is 1-2147483647, and 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 the default reference bandwidth.

Use **no auto-cost** to disable the bandwidth-based interface metric calculation.

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	Sets the cost of the interface.
show ipv6 ospf	Shows the OSPFv3 routing process information.

34.1.6 clear ipv6 ospf process

This command is used to clear and restart the OSPF instance.

clear ipv6 ospf [*process-id*]

Parameter description

Parameter	Description
process-id	Specify the ospf process id, <1-65535>

Command mode

Privileged mode.

Usage guidelines

In normal case, it is not necessary to use this command.

Examples	The example below restarts the OSPF instance.
	`en`
	`clear ipv6 ospf process`

34.1.7 default-metric

Use this command to set the default metric for route redistribution. Use the **no** form of this command to restore the default setting.

default-metric *metric-value*

no default-metric

Parameter description

Parameter	Description
metric-value	Default metric for route redistribution. Its range is 1-16777214, and the default value is 20.

Default configuration	20
Command mode	OSPFv3 configuration mode.
Usage guidelines	This command can be used with **redistribute** to set the default metric for route redistribution. But this command does not applies 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 route redistribution to 10. `default-metric 10`

Related commands

Command	Description
redistribute	Sets the redistribution of the routing information.
show ipv6 ospf	Shows the OSPFv3 routing process information.

34.1.8 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

This function is 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 neighboring relationship in between.

After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3. To disable some prefix information from being advertised, use **ipv6 ospf prefix-filter**.

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	Filters the prefix information to be advertised.
ipv6 router ospf	Starts the OSPFv3 routing process.
passive-interface	Sets the passive interface.
show ipv6 ospf interface	Shows the OSPFv3 interface information.

34.1.9 ipv6 ospf cost

Use this command to set the cost of the interface. Use the **no** form of this command to restore 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 1-65535, and the default value is 10.
instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

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. If **no auto-cost** is used, the default cost of the interface will be used.

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
```

	Command	Description
Related commands	**auto-cost**	Sets the reference bandwidth for interface metric.
	show ipv6 ospf interface	Shows the OSPFv3 interface information.
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

34.1.10 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 hello message from the neighbor, it considers that the neighbor fails. Use the **no** form of this command to restore 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 1-65535(s).
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

Default configuration	Four times the value of **ip ospf hello-interval**.
Command mode	Interface configuration mode.
Usage guidelines	The dead time between neighbors shall be the same. Otherwise they cannot establish normal adjacency. By default, the dead interval is four times the value of hello interval. If the hello interval is modified, the dead interval will be changeed accordingly. It's not recommended to modify the parameters directly. If needed, please be noted: 1. The dead interval shall be longer than the hello interval sent by the neighbor. 2. The same dead interval shall be set between 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	Sets the interval for the interface to send Hello packet.
show ipv6 ospf interface	Shows the OSPFv3 interface information.
instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

34.1.11 ipv6 ospf hello-interval

Use this command to set the interval for the interface to send Hello packet. Use the **no** form of this command to restore 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 Hello packet. Its range is 1-65535(s).
instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

Default configuration

10 seconds

Command mode

Interface configuration mode.

Usage guidelines

The same hello interval shall be set between the neighbors, otherwise they cannot establish normal adjacency.

Examples

The following example sets the interval for the interface to send Hello packet to 20s.

```
ipv6 ospf hello-interval 20
```

	Command	Description
Related commands	**ipv6 ospf dead-interval**	Sets the interval for the interface to consider that the neighbor fails.
	show ipv6 ospf interface	Shows the OSPFv3 interface information.
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

34.1.12 ipv6 ospf neighbor

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

ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [**poll-interval** <0-4294967295> | **priority** <0-255>]] [**instance** *instance-id*]

no ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [**poll-interval** <0-4294967295> | **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, not defined by default, where the cost configured on the interface will be used. Only the point-to-multipoint network type supports this option.
	poll-interval <*0-4294967295*>	(Optional) neighbor polling interval, in seconds, 120 s by default. Only the non-broadcast (NBMA) network type supports this option.
	priority <*0-255*>	(Optional) configure the priority of non-broadcast network neighbors, 0 by default. Only the non-broadcast (NBMA) network type supports this option.
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity

Command mode	Interface configuration mode.
Usage	You can set relevant parameters for the neighbor depending on the

guidelines	actual network type.

34.1.13 ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore 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	Specifies the broadcast network type.
non-broadcast	Specifies the non-broadcast network type.
point-to-point	Specifies the point-to-point network type.
point-to-multipoint	Specifies the point-to-multipoint network type.
point-to-multipoint non-broadcast	Specifies the point-to-multipoint non-broadcast network type.
instance *instance-id*	It will configure the interface-specified OSPFv3 entity

Default configuration	Broadcast 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	Sets the interface priority.
show ipv6 ospf	Shows the OSPFv3 interface information.

	interface	
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

34.1.14 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 0-255, and the default value is 1.
instance *instance-id*	It will configure the interface-specified OSPFv3 entity

Default configuration

1

Command mode

Interface configuration mode.

Usage guidelines

In the broadcast type, it is necessary to elect DR/BDR. In electing the DR/BDR, the router of the highest priority firstly becomes DR/BDR.. If several routers are of the same priority, the one with the largest Router-ID firstly becomes DR/BDR.

The router with the priority level of 0 does not participate in the election of DR/BDR.

If DR and BDR are available in the network, the modifying of 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 DR/BDR.

```
ipv6 ospf priority 0
```

Related

Command	Description

commands	**ipv6 ospf network**	Sets the network type of the interface.
	router-id	Sets the ID of the router.
	show ipv6 ospf interface	Shows the OSPFv3 interface information.
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

34.1.15 ipv6 ospf retransmit-interval

Use this command to set the interval for the interface to retransmit LSA. Use the **no** form of this command to restore 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 LSA. Its range is 1-65535(s).
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

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 LSA to 10s. `ipv6 ospf retransmit-interval 10`

Related	Command	Description

commands	**timers pacing retransmission**	Sets the interval for retransmitting LSA message.
	show ipv6 ospf interface	Shows the OSPFv3 interface information.
	show ipv6 ospf retransmission-list	Shows the neighbor LSA retransmission list of the OSPFv3 process.
	instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

34.1.16 ipv6 ospf transmit-delay

Use this command to set the delay for the interface to sending LSA. Use the **no** form of this command to restore 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 1-65535(s).
instance *instance-id*	It will configure the interface-specified OSPFv3 entity.

Default configuration

1 second

Command mode

Interface configuration mode.

Usage guidelines

Use this command to set the delay for the interface to transmit LSA.

Examples

The following example sets the delay for the interface to transmit LSA.

```
ipv6 ospf transmit-delay 2
```

Related commands

Command	Description
show ipv6 ospf interface	Shows the OSPFv3 interface information.

34.1.17 ipv6 router ospf

Use this command to start OSPFv3 routing process. Use the **no** form of this command to disable OSPFv3 routing process.

ipv6 router ospf *process-id*

no ipv6 router ospf *process-id*

Parameter description

Parameter	Description
process-id	OSPF process ID

Default configuration

Disabled the OSPFv3 route process.

Command mode

Global configuration mode.

Usage guidelines

After the OSPFv3 process is started, the OSPFv3 configuration mode is entered.

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	Shows the OSPFv3 routing process information.

34.1.18 max-concurrent-dd

Set the maximum number of DD packets that can be processed concurrently.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter description

Parameter	Description
number	Maximum number of packets

Default configuration

No restriction.

Command mode	OSPFv3 configuration mode.

Examples	The following example set max-concurrent-dd to 4 to allow interaction DD packets with only 4 neighbors concurrently:
	`router ipv6 ospf 1`
	`max-concurrent-dd 4`

34.1.19 passive-interface

Use this command to set the passive interface. Use the **no** form of this command to cancel the setting.

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	No passive interface is set.
Command mode	OSPFv3 configuration mode
Usage guidelines	After an interface is set to passive one, it no longer receives or sends 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

Command	Description

commands	**ipv6 ospf area**	Configure the interface to participate in the OSPFv3 routing process.
	show ipv6 ospf	Shows the OSPFv3 routing process information.
	show ipv6 ospf neighbor	Shows the OSPFv3 neighbor information.

34.1.20 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 *protocol* [**metric** *metric-value*] [**metric-type** *type-value*][**route-map** *map-tag*]

no redistribute *protocol* **[metric][metric-type][route-map]**

Parameter description

Parameter	Description
protocol	Routing protocol that is redistributed. Including static, connect, rip, isis, and bgp)
metric *metric-value*	Metric for the route redistribution. Its range is 1-16777214, and the default value is **default-metric**.
metric-type *type-value*	Metric type for the route redistribution. The default value is 2.
route-map *map-tag*	Routing policy associated with the route redistribution. It can be up to 32 characters. By default, **route-map** is not set.

Default configuration	This function is 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.

Examples

The following example redistributes the direct route and sets the metric for route redistribution to 100.

```
redistribute connect metric 100
```

Related commands

Command	Description
default-information originate	Sets the redistribution of the default route.
default-metric	Sets the default metric for route redistribution.
summary-prefix	Sets the summarized address range of the external route.
show ipv6 ospf	Shows the OSPFv3 routing process information.
show ipv6 ospf database	Shows the OSPFv3 LSA information.

34.1.21 router-id

Use this command to set the router ID. Use the **no** form of this command to delete the setting or restore the default router ID.

router-id *router-id*

no router-id

Parameter description

Parameter	Description
router-id	ID of the router. It is 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 router 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 need be reconfigured, shut down and restarts the OSPFv3 process, and then configure router ID.

Examples

The following example sets the ID of the router that participates in the OSPFv3 process to 1.1.1.1.

```
router-id 1.1.1.1
```

Related commands

Command	Description
ipv6 ospf priority	Sets the interface priority.
show ipv6 ospf	Shows the OSPFv3 routing process information.

34.1.22 timers spf

Use this command to set the delay for the OSPFv3 to perform SPF calculation after receiving the topology change and the interval between the two SPF calculations. The **no** format of this command is used to restore default.

timers spf *delay holdtime*

no timers spf

Parameter description

Parameter	Description
delay	The delay between the confirmation of the topology change and the starting of the SPF calculation. Its range is 0~214748364s, and the default value is 10s.
holdtime	The delay between the confirmation of the topology change and the starting of the SPF calculation. Its range is 0~214748364s, 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 resource the router uses.
Examples	`timers spf 2 4`

Related commands

Command	Description
clear ipv6 ospf	Restarts part of the OSPFv3 function.
show ipv6 ospf	Shows the OSPFv3 routing process information.

34.2 Showing Related Command

34.2.1 show ipv6 ospf

Show the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter description

Parameter	Description
process- id	OSPF process id

Command mode

Privileged mode.

Examples

The following example shows information about the OSPFv3 process.

```
DGS-3610# 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 router 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
```

Related commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
default-information originate	Sets the redistribution of the default route.
default-metric	Sets the default metric for route redistribution.
discard-route	Sets whether to add the discard route generated by the OSPF process to the kernel routing table.
distance	Sets the administrative distance for the OSPF to generate routing entries.
Router-id	Sets the OSPFv3 routing process ID.
timers pacint flood	Sets the interval for sending the LSA update message.
timers pacing lsa-group	Sets the interval for the OSPFv3 routing process to implement operations such as LSA refreshing, aging, checking, and calculation.
timers pacing retransmission	Sets the interval for retransmitting LSA message.
timers spf	Sets the delay for the OSPFv3 to perform SPF calculation after receiving the topology change and the interval between the two SPF calculations.

34.2.2 show ipv6 ospf database

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

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*	Shows the LSA information generated by the specified router.

Command mode

Privileged mode.

Examples

The following example shows information about the OSPFv3 process database.

```
DGS-3610# 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	Starts the OSPFv3 routing process.

34.2.3 show ipv6 ospf interface

Shows the OSPFv3 interface information.

show ipv6 ospf interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	Specifies interface type.

Command mode

Privileged mode.

Examples

The following commands show information about the OSPFv3 interface.

```
DGS-3610# 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
```

Related commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Starts the OSPFv3 routing process.

34.2.4 show ipv6 ospf neighbor

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
detail	Shows details about the neighbor.
interface-type interface-number	Specifies interface type.
neighbor-id	Specifies the neighbor router ID.

Command mode

Privileged .mode.

Examples

The following command shows the summary information about the OSPF neighbor.

```
DGS-3610# show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:33    FastEthernet 1/0
0
```

View the detailed information of OSPF neighbor via following commands:

```
DGS-3610# 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
```

Related commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.
area virtual-link	Configures the OSPFv3 virtual link.
show ipv6 ospf interface	Shows the OSPFv3 interface information.

34.2.5 show ipv6 ospf route

Shows the OSPFv3 neighbor information.

show ipv6 ospf [*process- id*] **route**

Parameter description

Parameter	Description
process- id	OSPFv3 process number

Command mode

Privileged mode.

Examples

The following information shows information about OSPF routing.

```
DGS-3610# 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	Starts the OSPFv3 routing process.

34.2.6 show ipv6 ospf topology

Show topology of each area of OSPFv3.

show ipv6 ospf [*process- id*] **topology** [**area** *area-id*]

Parameter description

Parameter	Description
process- id	OSPFv3 process number
area-id	Specified area

Command mode

Privileged mode.

Examples

The following command shows the topology of each area of OSPFv3.

```
DGS-3610# 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   --
```

Related commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
area range	Configures the address range of the OSPF area

34.2.7 show ipv6 ospf virtual-links

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

Command mode

Privileged mode.

Examples

The following command shows information about the OSPFv3 virtual link.

```
DGS-3610# 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**	Starts the OSPFv3 routing process.
	area virtual-link	Configures the OSPFv3 virtual link.
	show ipv6 ospf neighbor	Shows the OSPFv3 neighbor information.

35 Configuring IGMP Commands

35.1 IGMP Configuration Task List

Use the following commands to configure routing protocols for management of multicast group:

- **clear ip igmp group**
- **clear ip igmp interface**
- **ip igmp access-group**
- **ip igmp immediate-leave group-list**
- **ip igmp last-member-query-count**
- **ip igmp last-member-query-interval**
- **ip igmp limit (interface configuration mode)**
- **ip igmp querier-timeout**
- **ip igmp query-interval**
- **ip igmp query-max-response-time**
- **ip igmp robustness-variable**
- **ip igmp ssm-map enable**
- **ip igmp ssm-map static**
- **ip igmp version**
- **ip igmp join-group**
- **ip igmp static-group**
- **ip igmp limit (global configuration mode)**
- **show ip igmp groups**
- **show ip igmp interface**

35.1.1 clear ip igmp group

This command is used to clear dynamic group member information obtained from response messages from the IGMP buffer.

Command Syntax	**clear ip igmp group**[*group-address* | *interface-type interface-number*]

Parameter description

Parameter	Description
None	Delete all group information.
group-address	32-bit IP multicast group address, namely Category D address. 8 bits are in one group, in decimal. Groups are separated with dots.
interface-type	Associate interface type
interface-number	Associate interface number

Command mode

Privileged mode.

Usage guidelines

The IGMP cache includes a list that contains the multicast groups added to the host in the subnet directly connected to it. If the device is also added a group, this group will be included in this list. To delete all the entries from the IGMP cache, use the **clear ip igmp group** command without parameters.

Examples

Delete all group entries:

```
DGS-3610# clear ip igmp group
```

Related commands

Command	Description
show ip igmp groups	
show ip igmp interface	

35.1.2 clear ip igmp interface

This command is used to clear the IGMP entry for the interface.

Command syntax

clear ip igmp interface *ifname*

Parameter description

Parameter	Description
ifname	Name of the interface
None	All interfaces

Default	None
Command mode	Privileged mode.
Usage guidelines	This command is used to clear information on the interface that is generated when IGMP is configured. The *ifname* parameter can be ignored.
Examples	`DGS-3610# clear ip igmp interface eth1`

35.1.3 ip igmp access-group

This command is used to control a multicast group on the interface. Adding **no** before this command will disable 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 1-99..

Default	Filtering conditions are not set.
Command mode	Interface mode.
Usage guidelines	The host can access and add some multicast groups to some specific interfaces in a subnet. These multicast groups can be controlled using **ip igmp access-group**.

Examples	In the following example, the host service can only add the group 225.2.2.2 to the interface Eth0.
	`DGS-3610# configure terminal`
	`DGS-3610(config)# access-list 1 permit 225.2.2.2 0.0.0.0`
	`DGS-3610(config)# interface ethernet 0`
	`DGS-3610(config-if)# ip igmp access-group 1`

35.1.4 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 packet upon receiving the leaving packet. 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 packet upon receiving the leaving packet. Instead, it directly remove this interface for this group 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. Of course, you must make sure each interface of these multicast groups have one group member only.

```
DGS-3610# configure terminal
DGS-3610(config)# interface ethernet 0
DGS-3610(config-if)# ip igmp immediate-leave group-list 34
DGS-3610(config-if)# exit
DGS-3610(config)# access-list 34 permit 225.192.20.0 0.0.0.255
```

Related commands

Command	Description
ip igmp last-member-query-interval	

35.1.5 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** packets. This command is used to configure the value of **last-member-query-count**. Use the **no** command to restore 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 query count of the last member. The range is <2-7>.

Default

The default value of **last member query count** is 2.

Command mode

Interface configuration.

Usage guidelines

When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **ip igmp last-member-query-count** plus a half of the response time. The device will delete information about this group member if no member report is received within the waiting time.

Examples

Set the value of query count of the last member to 3.

```
DGS-3610# configure terminal
DGS-3610(config)# interface ethernet 0
DGS-3610(config-if)# ip igmp last-member-query-count 3
```

35.1.6 ip igmp last-member-query-interval

Use this command to set the time interval of sending a group specific query. To use the default value, add **no** before this command.

Command syntax

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval

Parameter description

Parameter	Description
interval	The interval value ranges <10-255>, in 0.1 second.

Default	0.1s
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 **ip igmp last-member-query-count** plus a half of the response time. The device will delete information about this group member if no member report is received within the waiting time.

Examples	The following example sets the interval of sending group specific query information to 2 seconds:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface eth0`
	`DGS-3610(config-if)# ip igmp last-member-query-interval 200`

Related commands

Command	Description
ip igmp immediate-leave	

35.1.7 ip igmp limit (interface configuration)

Use this command to set the maximum number of **igmp states** at the interface. To cancel this configuration, use the **no** form.

Command syntax

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit

Parameter description

Parameter	Description
number	The allowed maximum number of IGMP states. The range is 1-2097152.
except *access-list*	(Optional) The excluded extended access list.

Default

This command is not configured by default and has no default value. You must specify a value for this command when configuring it.

Command mode	Interface configuration mode.
Usage guidelines	This command in global configuration mode limits the number of the IGMP group records. The member messages over the limit are not buffered and transmitted. This command can be used to configure every interface. The interface and global configurations can be performed separately. The member packets will be ignored if they exceed the interface or global configuration.
Examples	The following example sets the maximum number to 300: `DGS-3610(config-if)# ip igmp limit 300`

35.1.8 ip igmp query-interval

This command is used 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 1~18000.

Default	125 seconds
Command mode	Interface configuration mode.
Usage guidelines	The time of ordinary query can be changed by configuring the query interval of ordinary member.
Examples	Configure the query interval of ordinary member to 120s on the interface Ethernet 0. `DGS-3610(config-if)# ip igmp query-interval 120` Configure the query interval of ordinary member to the default value on the interface Ethernet 0.

```
DGS-3610(config-if)# no ip igmp query-interval
```

35.1.9 ip igmp query-max-response-time

This command is used to configure the maximum response interval. The **no** form can be used 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 1~240.

Default

10s.

Command mode

Interface configuration mode.

Usage guidelines

This command works only when IGMPv2 is being used. This command controls the interval of response to the query message by the respondent before the device deletes the group information.

Examples

Configure the query interval of the last member to 20s on the interface Ethernet 0.

```
DGS-3610(config-if)# ip igmp query-max-response-time 20
```

Configure the query interval of the last member to the default value on the interface Ethernet 0.

```
DGS-3610(config-if)# no ip igmp query-max-response-time
```

35.1.10 ip igmp query-timeout

This command is used to configure the timer interval of other enquirers. Use the **no** form to set the timer interval of other enquirers to the default value.

Command syntax

ip igmp query-timeout *seconds*

no ip igmp query-timeout

Parameter description

Parameter	Description
seconds	The timer interval of other enquirers, in second.

		The range is 60~300.

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 DGS-3610, the default value is set to 255s. This device becomes the enquirer if no query packet is received in this duration.

Examples Configure the timer interval of other enquirers to 200s on the interface Ethernet 0.

```
DGS-3610(config-if)# ip igmp query-timeout 200
```

Configure the timer interval of other enquirers to the default value on the interface Ethernet 0.

```
DGS-3610(config-if)# no ip igmp query-timeout
```

35.1.11 ip igmp robustness-variable

Use this command to change the value of the enquirer robustness variable. To restore the default value, directly add **no** before the command.

Command syntax

ip igmp robustness-variable *number*

no ip igmp robustness-variable

Parameter description

Parameter	Description
number	The value of robustness variable, ranging <2-7>.

Default The default value is 2.

Command mode Interface configuration mode.

Examples The following example sets the value of robustness variable to 3:

```
DGS-3610# configure terminal
DGS-3610(config)# interface ethernet 0
```

```
DGS-3610(config-if)# ip igmp robustness-variable 3
```

35.1.12 ip igmp version

Use this command to set the version number of IGMP to be used on the interface. To use the default value, use the **no** form.

Command syntax

ip igmp version {**1** | **2** | **3**}

no ip igmp version

Parameter description

Parameter	Description
{**1** | **2** | **3**}	Three version numbers, ranging <1-3>.

Default

The version number is 2 by default.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to globally configure the maximum number of IGMP states of the IGMP, IGMPv3lite and URD reports. The part of the member packets that exceeds the threshold will not be saved in the IGMP cache and will not be forwarded.

This command can be used to configure every interface. The interface and global configurations can be performed separately. The member packets will be ignored if they exceed the interface or global configuration.

Examples

The following example sets the version number to 2:

```
DGS-3610# configure terminal
DGS-3610(config)# interface ethernet 0
DGS-3610(config-if)# ip igmp version 2
```

Related commands

Command	Description
ip igmp access-group	
ip igmp limit	
ip multicast rate-limit	

35.1.13 ip igmp join-group

This command configures the switch interface as 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 if you want to add an interface to a group. If the **no** option is used, the switch is not added to the multicast group.

Command Syntax	ip igmp join-group *group-address* **no** ip igmp join-group *group-address*

Parameter description

Parameter	Description
group-address	Multicast group address

Default configuration	The interface is not manually added to the multicast group by default.
Command mode	Interface configuration mode.
Usage guidelines	This command enables the host activities function of 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 of the interface is enabled, the host action on the interface can send the report packet, so that the interface can learn the configured group members. You can use this command if you want to add a group member to an interface.

Examples	Add a host group member manually:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface fast 0/1`
	`DGS-3610(config-if)# ip igmp join-group 233.3.3.3`

35.1.14 ip igmp static-group

This command directly adds the interface to a group. You can use this command if you want to add an interface to a group. If the **no** option is used, the switch is not added to the multicast group.

Command Syntax	ip igmp static-group *group-address* **no ip igmp static-group** *group-address*

Parameter description

Parameter	Description
group-address	Multicast group address

Default configuration	The switch is not added to the multicast group.
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 if you want to add an interface to a group.

Examples	Add a host group member manually:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface fast 0/1`
	DGS-3610(config-if)# **ip igmp static-group** *233.3.3.3*

35.1.15 ip igmp limit (global configuration)

Use this command to globally set the maximum number of generating **igmp** group record. To cancel this configuration, use the **no** form.

Command syntax	**ip igmp limit** *number* [**except** *access-list*] **no ip igmp limit** *number* [**except** *access-list*]

Parameter description

Parameter	Description
number	The allowed maximum number of IGMP states. The range is 1-2097152.
except	(Optional) Exclude the access-list from igmp limit.
access-list	(Optional) The excluded extended access list.

Default

This command is not configured by default. Because this command has no default value, you must specify a value for it when configuring this command.

Command mode

Global configuration mode.

Usage guidelines

Use this command to globally configure the maximum number of IGMP group record. The part of the member packets that exceeds the threshold will not be saved in the IGMP cache and will not be forwarded.

This command can be used to configure every interface. The interface and global configurations can be performed separately. The member packets will be ignored if they exceed the interface or global configuration.

Examples

The following example sets the maximum number to 300:

```
DGS-3610(config) # ip igmp limit 300
```

35.1.16 ip igmp proxy-server

This command starts the service function of all downlink **mroute-proxy** ports. If you configure this command on an interface, the interface becomes the uplink port of the corresponding **mroute-proxy**, associates its downlink ports, and maintains the group information reported by the downlink ports.

ip igmp proxy-server

no ip igmp proxy-server

Default configuration

All interfaces are not in the proxy-server state.

Command mode	Interface configuration mode

Usage guidelines	The command can configure at most 32 interfaces. Each proxy-server port can associate with the maximum of 255 downlink ports. When receiving a query message, the proxy-server port responds according to the member information maintained by the port itself. The member information maintained by the proxy-server port is collected from the interface configured with mroute-proxy. Therefore, if a port is configured with proxy-server, the port performs the host activities, but not the router activities. If you run switchport on a port for other ports, the ip igmp mroute-proxy interface command configured on the associated downlink ports is automatically deleted.

Examples	Configure a port to the **proxy-server** module: `DGS-3610(config-if)# ip igmp proxy-server`

35.1.17 ip igmp mroute-proxy

After this command is configured for a port, the port can transmit messages to its uplink ports.

ip igmp mroute-proxy *interfname*

no ip igmp mroute-proxy

Parameter description

Parameter	Description
interfname	Name of the uplink interface

Default configuration	This function is not configured.

Command mode	Interface configuration mode

Usage guidelines	After an uplink interface is configured as proxy-server port, the interface can transmit the IGMP messages sent by its members.

Examples	Configure an interface to **mroute-proxy** port: `DGS-3610(config-if)# ip igmp mroute-proxy fa 0/1`

35.1.18 ip igmp ssm-map enable

This command starts the **igmp ssm-map** function in the global mode. The command format is:

ip igmp ssm-map enable

no ip igmp ssm-map enable

Default configuration	The function is not enabled.
Command mode	Global configuration mode.
Usage guidelines	If this command is configure, 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 mode: DGS-3610(config)# **ip igmp ssm-map enable**

35.1.19 ip igmp ssm-map static

This command maps the static **ssm-map** source record in the global mode. The command format is:

ip igmp ssm-map static *access-list a.b.c.d*

no ip igmp ssm-map static *access-list a.b.c.d*

Parameter description

Parameter	Description
access-list	The range of ACL number is 1–99
a.b.c.d	Unicast address mapped in group record

Default configuration	The source address is not mapped.
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 all received messages below v3 to the corresponding source records.
Examples	Map all group records with ACL 11 to the source address 192.168.2.2: `DGS-3610(config)# ip igmp ssm-map static 11 192.168.2.2.`

35.1.20 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 groups [*group-address* | *interface-type interface-number*] [**detail**]

Parameter description

Parameter	Description
group-address	32-bit IP multicast group address, namely Category D address. 8 bits are in one group, in decimal. Groups are separated with dots.
interface-type	Associate interface type
interface-number	Associate interface number
detail	Show detailed information
None	Show information about all the groups

Default

Command mode

User mode or Privileged mode.

Usage guidelines

Use this command without any parameter 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:

```
DGS-3610# 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:

```
DGS-3610# 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
```

35.1.21 show ip igmp interface

Use this command to view configuration information of this interface.

Command syntax

Show ip igmp interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Associate interface type
interface-number	Associate interface number
None	Show information about all the interfaces

Default	
Command mode	User mode or Privilege mode.

Examples	The following example shows status information of all the interfaces:
	`DGS-3610# show ip igmp interface`
	`Interface vlan1.1 (Index 4294967295)`
	`IGMP Active, Non-Querier, Version 3 (default)`
	`IGMP querying router 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`

35.1.22 show ip igmp ssm-mapping

This command shows the **ssm-map** information of the IGMP configuration. The command format is:

show ip igmp ssm-mapping *(A.B.C.D |)*

Parameter description

Parameter	Description
A.B.C.D	Mapped source address

Default configuration	The ssm-map information of all IGMP configurations is displayed.
Command mode	Global configuration mode.
Usage guidelines	If all the parameters are not used, the related configurations are displayed.

Examples

Show the **ssm-map** configuration information:

```
DGS-3610# sh ip igmp ssm-mapping

SSM Mapping: Enabled

Database   : Static mappings configured
```

Show the group information 233.3.3.3 of being mapped

```
DGS-3610#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
```

36 PIM-DM Configuration Command

36.1 PIM-DM Related Configuration Commands

PIM-DM protocol configuration includes following commands:

- **ip pim dense-mode**
- **ip pim neighbor-filte**
- **ip pim query-interval**
- **ip pim state-refresh disable**
- **ip pim state-refresh origination-interval**
- **show ip pim interface**
- **show ip pim neighbor**

36.1.1 ip pim dense-mode

To enable PIM-DM on the current interface, use the **ip pim dense-mode** command. Use the **no** form of this command to disable PIM-DM on the current interface.

ip pim dense-mode

no ip pim dense-mode

Parameter description	This command has no parameters.
Default configuration	PIM-DM is not enabled.
Command mode	Interface configuration mode.
Examples	DGS-3610# **configure terminal** DGS-3610(config)# **interface fastethernet** *0/0*

```
DGS-3610(config-if)# ip pim dense-mode
```

Note

You must enable the multicast route transmit function before starting the PIM-SM. Otherwise, the interface cannot transmit multicast packets even the PIM-SM is enabled.

When the PIM-SM is enabled, the IGMP is automatically enabled on the interfaces.

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-configure this command.

During the configuration of this command, if the prompt "PIM-DM Configure failed! VIF limit exceeded in NSM!!!" appears, it indicates the allowed interface configurations exceed the upper limit of the multicast interfaces. In this case, delete the unnecessary PIM-SM or DVMRP interfaces.

36.1.2 ip pim neighbor-filter

To enable the neighbor filtering on the interface, use the **ip pim neighbor-filte**r command. 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 refused 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	Name of number-form or name-form access list.

Default configuration

The neighbor filtering function is not enabled for the interface.

Command mode

Interface configuration mode.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# interface fastethernet 0/0
```

```
DGS-3610(config-if)# ip pim neighbor-filter 14
```

Note

Description of the **ip pim neighbor-filter** command:

1. When the associated ACL rule is permitted, 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.

36.1.3 ip pim query-interval

To configure the **hello interval** value again, use the **ip pim query-interval** command.

The **no** form of this command is used to clear **hello interval**.

ip pim query-interval *seconds*

no ip pim query-interval

Parameter description

Parameter	Description
seconds	An integer in <1-65535>, in second.

Default configuration

30 seconds.

Command mode

Interface configuration mode.

Usage guidelines

If **hello interval** is set, the **hello holdtime** value be updated to a value 3.5 times of **hello interval**.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# interface fastethernet 0/0
DGS-3610(config-if)# ip pim hello-interval 123
```

36.1.4 ip pim state-refresh disable

To prohibit the interface from processing and forwarding PIM dense mode status update messages, use the **ip pim state-refresh disable** command. The **no** form of this command is used to restore the PIM-DM status update function of the interface.

ip pim state-refresh disable

no ip pim state-refresh disable

Parameter description	None
Default	The update message is processed and forwarded by default.
Command mode	Global configuration mode.
Usage guidelines	When it is prohibited to process and forward the status update packets, the sent Hello packet does not contain the status update option, the SR Cap field will not be processed when the Hello packet is received, and the status update packet will not be processed.

Examples	The following example disables the processing of the PIM dense-mode status update message.
	`DGS-3610# configure terminal`
	`DGS-3610(config)# ip pim state-refresh disable`

Caution

Description of the **ip pim state-refresh disable** command:

Generally, it is not recommended to disable the status update 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.

36.1.5 ip pim state-refresh origination-interval

To set the originating time interval of the status update message of PIM-DM again, use the **ip pim state-refresh origination-interva**l command. The originating time interval is the seconds elapsed between two status update messages. The **no** form of this command resets the originating time interval to the default value.

ip pim state-refresh origination-interval *seconds*

no ip pim state-refresh origination-interval

Parameter description

Parameter	Description
seconds	An integer in <1-100>, in second.

Default configuration

60 seconds.

Command mode

Interface configuration mode.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# interface fastethernet 0/0
DGS-3610(config-if)# ip pim state-refresh
origination-interval 65
```

36.1.6 show ip pim dense-mode interface

To show information about the PIM-DM interface, use the **show ip pim dense-mode interface** command.

show ip pim dense-mode interface [*interface-type interface-number*] [**detail**]

Parameter description

Parameter	Description
interface-type interface-number	The interface type and interface ID.
detail	Show details of interface

Default

If no interface is specified, information about all the PIM interfaces will be displayed.

Command mode

User Mode

Privileged EXEC mode

Examples

Shown below is the output of the **show ip pim dense-mode interface** command:

```
DGS-3610# show ip pim dense-mode interface
Address:   Interface  VIFIndex  Ver/Mode    Nbr Count
192.168.1.53/24 wm0   0          v2/D          2
192.168.10.53/24 wm1  2          v2/D          0
```

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
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 information about neighbors of the PIM-DM interface

36.1.7 show ip pim dense-mode neighbor

To show information about the PIM-DM neighbor, use the **show ip pim dense-mode neighbor** command.

show ip pim dense-mode neighbor [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	The interface type and interface ID.

Command mode

User EXEC Mode

Privileged mode.

Examples

Shown below is the output of the **show ip pim dense-mode neighbor** command:

```
DGS-3610# show ip pim dense-mode neighbor
Neighbor-Address  Interface    Uptime/Expires      Ver
192.168.1.152      wm0         17:15:42/00:01:28    v2
192.168.1.149      wm0         17:15:34/00:01:34    v2
```

37 Configuring PIM-SM Commands

37.1 PIM-SM Configuration Command List

PIM-SM protocol configuration includes following commands:

- **clear ip mroute pim**
- **clear ip pim sparse-mode bsr rp-set ***
- **ip pim bsr-candidate**
- **ip pim dr-priority**
- **ip pim query-interval**
- **ip pim jp-timer**
- **ip pim neighbor-filter**
- **ip pim register-rate-limit**
- **ip pim register-rp-reachability**
- **ip pim register-source**
- **ip pim register-suppression**
- **ip pim rp-address**
- **ip pim rp-candidate**
- **ip pim rp-register-kat**
- **ip pim sparse-mode**
- **ip pim spt-threshold**
- **ip pim spt-threshold group-list**
- **ip pim ssm**
- **show debugging pim sparse-mode**
- **show ip pim sparse-mode mroute**
- **show ip pim sparse-mode bsr-router**
- **show ip pim sparse-mode interface**
- **show ip pim sparse-mode interface detail**
- **show ip pim sparse-mode neighbor**

- **show ip pim sparse-mode neighbor detail**
- **show ip pim sparse-mode nexthop**
- **show ip pim sparse-mode rp-hash**
- **show ip pim sparse-mode rp mapping**
- **show memory pim sparse-mode**

37.1.1 ip pim bsr-candidate

Command syntax

ip pim bsr-candidate *interface-type interface-number* [**hash**][**priority**]

Parameter description

Parameter	Description
interface-type terface-number	Specify an interface
hash	The range is <0-32>. Configure the hash madk length for the RP election mechanism.
priority	The range is <0-255>. Configure the priority parameter for the candidate BSR.

Default

None

Command mode

Global configuration mode.

Usage guidelines

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 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

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim bsr-candidate eth0 20 30
```

37.1.2 ip pim dr-priority

Command syntax

ip pim dr-priority *priority*

Parameter description

Parameter	Description
priority	The larger the priority value, the higher the priority. The range is <0-4294967294>. The default value is 1.

Default

The default value is 1

Command mode

Interface configuration mode.

Usage guidelines

The following apply when a DR is selected:

- When a higher priority is set for a device, it may be elected as DR. If several multicast devices have the same DR, the device with the largest IP address is elected as DR.
- When the priority parameter in the hello message is not set for a device, this device is considered to have the highest priority and may be elected as DR. If several devices are in this status, the device with the largest IP address will be elected as DR.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# interface eth0
DGS-3610(config-if)# ip pim dr-priority 11234
```

Related commands

Command	Description
ip pim ignore-rp-set-priority	

37.1.3 ip pim query-interval

Command syntax

ip pim query-interval *interval*

Parameter description

Parameter	Description
interval	The range is <1-65535>, in second.

Default

30s

Command mode

Interface configuration mode.

Usage guidelines

After the query-interval value is configured, holdtime will be changed to 3.5*hello-interval if it is smaller than 3.5*query-interval.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# interface eth0
DGS-3610(config-if)# ip pim query-interval 123
```

Related commands

None

37.1.4 ip pim jp-timer

Command syntax

ip pim jp-timer interval

Parameter description

Parameter	Description
interval	1-65535, in second.

Default

60s

Command mode

Global configuration mode.

Usage guidelines

Set the time interval of sending join/prune regularly.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim jp-timer 234
```

37.1.5 ip pim neighbor-filter

Command syntax

ip pim neighbor-filter *access_list*

Parameter description

Parameter	Description
access_list	access-list: The range of supported number-based ACL is 1-99. Name-based ACL is also supported.

Default

The neighbor filtering function is not enabled for the interface.

Command mode

Interface configuration mode.

Usage guidelines

Set the neighbor filtering that will enhance the security of the PIM network and provide neighbor restriction. As long as a neighbor is denied by the filtering access list, PIM-SM will not establish peering relationship with this neighbor, or will terminate established peering relationship with this neighbor.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# interface eth0
DGS-3610(config-if)# ip pim neighbor-filter 14
DGS-3610(config-if)# exit
DGS-3610(config)# ip access-list deny 192.168.1.53
DGS-3610(config)# ip access-list permit anyip pim
register-rate-limit
```

Command syntax

ip pim register-rate-limit <*1-65535*>

Parameter description

Parameter	Description
<1-65535>	The maximum number of register packets that can be sent per second

Default

No restriction.

Command mode

Global configuration mode.

Usage guidelines

This command is used to configure each (S, G) status, not the bandwidth of the system. Using this command will restrict the load of DR and RP when the number of incoming register packets exceeds the limit. This command is only used in the PIM-SM (S, G) entity.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim register-rate-limit 3444
```

37.1.6 ip pim register-rp-reachability

Command syntax

ip pim register-rp-reachability

Parameter description

None

Default

None

Command mode

Global configuration mode.

Usage guidelines

This command is used to judge whether the source of the register packet is reachable. If not reachable, this register packet is not processed.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim register-rp-reachability
```

37.1.7 ip pim register-source

Command syntax

ip pim register-source {*source_ip* | *interface-type interface-number*}

Parameter description

Parameter	Description
source_ip	Specify the source ip address of the register packet
interface-type interface-number	Specify the interface whose IP address is used as the source IP address in the register packet

Default

No configuration

Command mode

Global configuration mode.

Usage guidelines

This command should be used when the source IP address of the register message is not sent by the unique RP. This case occurs when the source address is filtered or the source address is not unique and the response message from RP cannot be sent to DR successfully.

The configured address must be reachable. When RP sends a correct Register-Stop message, it will respond accordingly. Therefore, it is recommended to use the loopback address of the interface, or other physical address.

Note: This configuration does not require that PIM has been started.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim register-source 3.3.3.3
```

37.1.8 ip pim register-suppression

Command syntax

ip pim register-suppression *<1-65535>*

Parameter description

Parameter	Description
<1-65535>	Suppression time, in seconds.

Default 60 seconds.

Command mode Global configuration mode.

Usage guidelines Configuring this value will change the register packet suppression time defined on DR. if the **ip pim rp-register-kat** command is not configured, defining this value on RP will modify the period of RPkeepalive.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim register-suppression
```

37.1.9 ip pim rp-address

Command syntax **ip pim rp-address** *A.B.C.D* [*access_list*]

Parameter description

Parameter	Description
A.B.C.D	ip address of RP
access_list	access-list: The ranges of supported number-based acl are 1-99 and 1300-1999. Name-based acl is also supported.

Default None

Command mode Global configuration mode.

Usage guidelines This system supports configuration of multicast static RP, as well as configuration of both the static RP and BSR mechanisms. When you use this command, note that:

- If both the BSR mechanism and the RP static configuration are effective, the RP static configuration takes precedence.
- When statically configure the RP address using the control list, you can configure several multicast groups (using ACL) or all the multicast groups (not using ACL). However, one RP static address cannot be used in several configuration processes.

- If multiple addresses can be configured for RP, the larger address will be used first.
- Only the address that can be filtered as defined in ACL indicates an invalid multicast group. The default address 0.0.0.0/0 to be filtered is considered to filter all the multicast groups 224/4.
- After configuration is finished, the static RP source address is inserted to the group range-based static RP group tree structure. Each group range multicast static group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IP address. When a RP is selected for a group range, the first element, namely the one wit the largest IP address, will be selected first.
- Deleting a RP static address also deletes this address from all the existing groups and selects an address from the addresses in the existing tree structure as the RP address.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim rp-address 3.3.3.3 4
```

37.1.10 ip pim rp-candidate

Command syntax

ip pim rp-candidate *interface-type interface-number [priority][interval][group_list]*

Parameter description

Parameter	Description
interface-type interface-number	Interface
priority	The range is <0-255>
interval	The range is <0-16383>
group_lis	The range of supported number-based ACL is 1-99. Name-based ACL is also supported.

Default

None

Command mode

Global configuration mode.

Usage guidelines

In the PIM-SM protocol, the shared tree RPT created by the route multicast data uses the Rendezvous Point (RP) as the root and the group member as the leaf. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends unicast C-RP messages to BSR regularly, and BSR spreads the messages throughout the PIM domain.

If the interface needs to be specified as the candidate rp in a special range of group, this command can carry the **acl**. Noted that the calculation of the range of group only bases on the **ace** of **permit**, it doesn't perform the integration calculation for the **ace** of **deny**.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim rp-candidate eth0 priority 3 group-list
3
```

37.1.11 ip pim rp-register-kat

Command syntax

ip pim rp-register-kat *<1-65535>*

Parameter description

Parameter	Description
<1-65535>	Set the time value of the KAT timer, in second.

Default

210s

Command mode

Global configuration mode.

Usage guidelines

Configure the **kat** interval of **rp**.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# ip pim rp-register-kat 3454
```

37.1.12 ip pim sparse-mode

Command syntax

ip pim sparse-mode

Parameter description	None
Default	pimsm is not enabled.
Command mode	Interface configuration mode.
Usage guidelines	Used to enable the **pim sm** command.

Examples	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface eth0`
	`DGS-3610(config-if)# ip pim sparse-mode`

Note

You must enable the multicast route transmiting function before starting the PIM-SM. Otherwise, the interface cannot transmit multicast packets even the PIM-SM is enabled.

When the PIM-SM is enabled, the IGMP is automatically enabled on the interfaces, it doen't need to configure manually..

During the configuration of this command, if the prompt "Failed to enable PIM-DM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-configure this command.

During the configuration of this command, if the prompt "PIM-SM Configure failed! VIF limit exceeded in NSM!!!" appears, it indicates the allowed interface configurations exceed the upper limit of the multicast interfaces. In this case, delete the unnecessary PIM-DM or DVMRP interfaces.

37.1.13 ip pim spt-threshold

Command syntax	**ip pim spt-threshold**

Parameter description	None
Default	None
Command mode	Global configuration mode.
Usage guidelines	Use this command when you want to enable the **rp** to **spt** tree conversion function.
Examples	DGS-3610# **configure terminal** DGS-3610(config)# **ip pim spt-threshold**

37.1.14 ip pim spt-threshold group-list

Command syntax	**ip pim spt-threshold group-list** *access_list*
Parameter description	**Parameter** / **Description** *access_list* / The ranges of supported number-based ACL are1-99, and 1300-1999. Name-based ACL is also supported.
Default	None
Command mode	Global configuration mode
Usage guidelines	Use this command when you want to enable the RP-to-SPT tree conversion function for some groups.
Examples	DGS-3610# **configure terminal** DGS-3610(config)# **ip pim spt-threshold group-list** *LIST1* DGS-3610(config)# **ip access-list permit** *224.0.1.3*

37.1.15 ip pim ssm

Command syntax

ip pim ssm { **range | range** *access_list*}

Parameter description

Parameter	Description
defaul	The group range is: 232/8
access_list	The range of supported number-based ACL is 1-99. Name-based ACL is also supported.

Default

None.

Command mode

Global configuration mode.

Usage guidelines

Use this command when you want to enable pim-ssm or enable pim-ssm for some specific groups.

Examples

The following command sets the source-specific multicast with the access control list as 10.

```
access-list 10 permit 225.1.1.1
ip pim ssm range 4
```

Command syntax

clear ip mroute {*|*group_ip* |*group_ip* source_*ip* } **pim sparse-mode**

Parameter description

Parameter	Description
*	Delete all the pimsm multicast routing table entries.
group_ip	Delete the pimsm multicast routing table entries for specific groups.
group_ip source_ip	Delete the pimsm multicast routing table entries for specific group sources.

Default

None

Command mode	Privileged mode.
Usage guidelines	Delete pimsm multicast routing table entries manually
Examples	DGS-3610# **clear ip mroute * pim sparse-mode** DGS-3610# **clear ip mroute** *224.2.2.2* **pim sparse-mode** DGS-3610# **clear ip mroute** *224.2.2.2 2.2.2.2* **pim sparse-mode**
Related commands	None

37.1.16 clear ip pim sparse-mode bsr rp-set

Command syntax	**clear ip pim sparse-mode bsr rp-set ***

Parameter description

Parameter	Description
*	Clear all settings.

Default	None
Command mode	Privileged mode.
Usage guidelines	Manually delete all the RP information learnt dynamically.
Examples	DGS-3610# **clear ip pim sparse-mode bsr rp-set ***

37.1.17 show ip pim sparse-mode mroute

Command syntax	**show ip pim** sparse**-mode mroute** *{group_ip|source_ip|group_ip source_ip|source_ip group_ip}*

Parameter description

Parameter	Description
group_ip	A.B.C.D Group address.
source_ip	A.B.C.D Source address.

Default

None

Command mode

User/privileged mode.

Usage guidelines

Used to view routing information. Neither two group addresses nor two source addresses can be used at the same time.

Examples

```
DGS-3610# show ip pim sparse-mode mroute
DGS-3610# show ip pim sparse-mode mroute 40.40.40.11
DGS-3610# show ip pim sparse-mode mroute 235.0.0.1
DGS-3610# show ip pim sparse-mode mroute 235.0.0.1
40.40.40.11
```

The following output shows all the routing information:

```
DGS-3610# show ip pim sparse-mode mroute
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 1
(*, 224.0.1.3)
RP: 10.10.5.153
RPF nbr: 192.168.1.152
RPF idx: wm0
Upstream State: JOINED
Local ..............................
Joined ..j..........................
Asserted ...........................
FCR:
Source: 10.10.1.52
Outgoing ..o........................
KAT timer running, 144 seconds remaining
Packet count 1
```

37.1.18 show ip pim sparse-mode bsr-router

Command syntax	**show ip pim sparse-mode bsr-router**
Parameter description	None
Default	None
Command mode	User/privileged mode.
Usage guidelines	Used to view BSR information.
Examples	DGS-3610# **show ip pim sparse-mode bsr-router** PIMv2 Bootstrap information BSR address: 10.10.11.35 (?) Uptime: 00:00:38, BSR Priority: 0, Hash mask length: 10 Expires: 00:01:32 Role: Non-candidate BSR State: Accept Preferred

Related commands

Command	Description
show ip pim sparse-mode rp mapping	
show ip pim sparse-mode neighbor	

37.1.19 show ip pim sparse-mode interface

Command syntax	**show ip pim sparse-mode** *interface*
Parameter description	None
Default	None

Command mode	User/privileged mode.
Usage guidelines	View the PIM SM interface information.
Examples	DGS-3610# **show ip pim sparse-mode interface** AddressInterface VIFindexVer/Nbr DR DRMode CountPrior 192.168.1.53 wm0 0 v2/S 2 2 192.168.1.53 192.168.10.53 wm1 2 v2/S 0 2 192.168.10.53

37.1.20 show ip pim sparse-mode interface detail

Command syntax	**show ip pim sparse-mode interface detail**
Parameter description	None
Default	None
Command mode	User/privileged mode
Usage guidelines	View the PIM SM interface information.
Examples	DGS-3610# **show ip pim sparse-mode interface detail** eth1 (vif 3): Address 192.168.1.149, DR 192.168.1.149 Hello period 30 seconds, Next Hello in 15 seconds Triggered Hello period 5 seconds Neighbors: 192.168.1.22 eth2 (vif 0): Address 10.10.11.149, DR 10.10.11.149 Hello period 30 seconds, Next Hello in 18 seconds Triggered Hello period 5 seconds Neighbors: 10.10.11.4

37.1.21 show ip pim sparse-mode neighbor

Command syntax	**show ip pim sparse-mode neighbor**
Parameter description	None
Default	None
Command mode	Global/privileged mode.
Usage guidelines	Shows the neighbor information.
Examples	DGS-3610# **show ip pim sparse-mode neighbor** Neighbor Interface Uptime/Expires Ver DRAddress Priority/Mode 10.10.0.9 eth0 00:55:33/00:01:44 v2 1 / 10.10.0.136 eth0 00:55:20/00:01:25 v2 1 / 10.10.0.172 eth0 00:55:33/00:01:32 v2 1 / DR 192.168.0.100 eth1 00:55:30/00:01:20 v2 N / DR

37.1.22 show ip pim sparse-mode neighbor detail

Command syntax	**show ip pim sparse-mode neighbor detail**
Parameter description	None
Default	None
Command mode	User/privileged mode
Usage guidelines	Show details of PIM SM neighbor.

Examples

```
DGS-3610# show ip pim sparse-mode neighbor detail
Nbr 192.168.1.22 (eth1)
Expires in 93 seconds
Nbr 10.10.11.4 (eth2)
Expires in 83 seconds
```

37.1.23 show ip pim sparse-mode nexthop

Command syntax

show ip pim sparse-mode nexthop

Parameter description

None

Default

None

Command mode

Global/privileged mode.

Usage guidelines

View information about the next hop, including the interface number, address, metric and other information of the next hop.

Examples

```
DGS-3610# show ip pim sparse-mode nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination  Type  Nexthop  Nexthop  Nexthop  Nexthop  Metric
Pref    Refcnt
Num    Addr     Ifindex    Name

_____________________________________________________________
10.10.0.9      .RS.   1    0.0.0.0    4              0     0     1
192.168.35.10 .RS.   1    10.10.0.2  4     eth2     10    0     1
Field Description
Destination The destination address for which PIM-SM requires
nexthop information.
Type The type of destination, as indicated by the Flags description.
N = New, R=
RP, S = Source, U = Unreachable
Nexthop Num The number of nexthops to the destination. PIM-SM always
uses only 1 nexthop.
Nexthop Addr The address of the primary nexthop gateway
Nexthop IfIndex The interface on which the nexthop gateway can be
reached.
Nexthop Name The name of nexthop interface
Metric The metric of the route towards the destination
Preference The preference of the route towards destination
```

```
Refcnt Internal usage only (for debugging)
```

37.1.24 show ip pim sparse-mode rp-hash

Command syntax

show ip pim sparse-mode rp-hash *A.B.C.D*

Parameter description

Parameter	Description
A.B.C.D	Used as the hash for selecting a group address.

Default

None

Command mode

Global/privileged mode.

Usage guidelines

View RP information.

Examples

```
DGS-3610# show ip pim sparse-mode rp-hash 224.0.1.3
RP: 10.10.11.35
Info source: 10.10.11.35, via bootstrap
```

37.1.25 show ip pim sparse-mode rp mapping

Command syntax

show ip pim sparse-mode rp mapping

Parameter description

None

Default

None

Command mode

Global/privileged mode.

Usage guidelines

View mapping and RP information.

Examples

```
DGS-3610# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 10.10.0.9
Info source: 10.10.0.9, via bootstrap, priority 0
Uptime: 16:52:39, expires: 00:02:50
```

Related commands

Command	Description
show ip pim sparse-mode rp-hash	

38 Configuring Multicast Routing Commands

38.1 Configuring related commands:

- **clear ip mroute**
- **clear ip mroute statistics**
- **ip mroute**
- **ip multicast route-limit**
- **ip multicast ttl-threshold**
- **ip multicast-routing**
- **show ip mroute**
- **show ip rpf**
- **show ip mvif**

38.1.1 clear ip mroute

Use this command to remove the forwarding information in the IP multicast route in the route table.

clear ip mroute {***** | *group-address* [*source -address*]}

Parameter description

Parameter	Description
*	Remove the forwarding information in the IP multicast route table.
group-address	group-address of IP multicast route
source-address	Source-address of multicast routes.

Default

None

Command mode	Privileged mode.
Usage guideline	None
Examples	Following example is to clear the group address 230.0.0.0 entry in the multicast route table: `DGS-3610# clear ip mroute 230.0.0.0`

Related commands

Command	Description
show ip mroute	Show the multicast route forwarding information.

Platform description	None

38.1.2 clear ip mroute statistics

Use this command to remove the forwarding information in the IP multicast route in the route table.

clear ip mroute statistics {***** | *group-address* [*source -address*]}

Parameter description

Parameter	Description
*	Remove the forwarding information in the IP multicast route table.
group-address	group-address of IP multicast route
source-address	Source-address of multicast routes.

Default	None
Command mode	Privileged mode.
Usage guideline	This command allows you to clear the IP multicast routing statistics.

Examples	Following example is to clear the group address 230.0.0.0 entry in the multicast route table: `DGS-3610# clear ip mroute statistics 230.0.0.0`

Related commands	**Command**	**Description**
	show ip mroute	Show the multicast route forwarding information.

Platform description	None

38.1.3 ip mroute

Use this command to configure multicast static routes. Use the **no** form of this command to delete the configured routes.

ip mroute *source-address mask* [*protocol as-number*] {*rpf-addrress* | *interface-type interface-number*} [*distance*]

no ip mroute *source-address mask* [*protocol as-number*] {*rpf-addrress* | *interface-type interface-number*} [*distance*]

Parameter description

Parameter	**Description**
source-address	Multicast source address
mask	Mask of multicast source address
protocol	(Optional) the unicast routing protocol being used
rpf-address	Input interface of multicast route
interface-type interface-number	The interface type and interface ID.
distance	Management distance, used to determine whether to use the route for RPF routing. The default value is 0.

Default	*distance*: 0
Command mode	Global configuration mode.

Usage guideline	This command allows you to statically configure the source.

Examples	The following example configures all the sources in a network from passing 172.30.10.13:
	`DGS-3610(config)# ip mroute 172.16.0.0 255.255.0.0 172.30.10.13`
	The following example configures all sources to be reachable via the F1/1 interface:
	`DGS-3610(config)# ip mroute 224.0.0.0 255.255.255.255 FastEthernet 1/1`

Platform description	None

38.1.4 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 route-limit *limit* [*threshold*]

no ip multicast route-limit *limit* [*threshold*]

Parameter description

Parameter	Description
limit	The number of the entries that can be added to the multicast routing table is 1~2147483647. The default value is 1024.
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	None

Examples	The following example sets the route limit to 500. `DGS-3610(config)# ip multicast route-limit 500`
Platform description	None

38.1.5 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 the default value.

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

Parameter description

Parameter	Description
ttl-value	Set the TTL threshold of the interface, within the range of 0~255.

Default	The default *ttl-value* is 1.
Command mode	Interface configuration mode.
Usage guideline	Use **show running-config** to display configuration. A router 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. Please 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. `DGS-3610(config-if)# ip multicast ttl-threshold 5`
Platform description	None

38.1.6 ip multicast-routing

This command allows you to enable multicast routing forwarding. The **no** form of this command allows you to disable multicast routing forwarding.

ip multicast-routing

no ip multicast-routing

Default	Disabled
Command mode	Global configuration mode.
Usage guideline	This command allows you to enable multicast routing forwarding. Precautions: If this command is configured, the VLAN port, L2AP member port, and L3AP member port will change. You should first execute the N" form of the command, before you can restart multicast routing forwarding.
Examples	This command enables multicast routing forwarding. `DGS-3610(config)# ip multicast-rounting`
Platform description	None

38.1.7 ip multicast-rpf

This command allows you to configure the RPF check mode of the equipment. The **no** form of this command allows you to restore the default configuration.

ip multicast-rpf

no ip multicast-rpf

default ip multicast-rpf

Default	SVI-based check mode
Command mode	Global configuration mode.

Usage guideline	None
Examples	The following example configures multicast RPF check as the routed port check mode. `DGS-3610(config)# ip multicast-rpf routed-port`
Platform description	None

38.1.8 show ip mroute

This command allows you to show the multicast forwarding table.

show ip mroute [*group-address*] [*source-address*] [**summary**] [**count**]

Parameter description

Parameter	Description
group-address	Multicast routing group address
source-address	Multicast routing source address
summary	Show the summary of the multicast routing table.
count	Show the count of the multicast routing table.

Default	None
Command mode	Privileged mode.
Usage guideline	None

Examples	The following example shows the information of all multicast routing tables:
	`DGS-3610# 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 multicast routing table:

```
DGS-3610# 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:

```
DGS-3610# 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:

```
DGS-3610# 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 T-Timed F-Already set to the forwarding table
Timers:Uptime/Stat Expiry	Time when the entry is created/ the time when it expires
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 the input 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

	Command	**Description**
Related commands	**ip multicast-routing**	Enabling Multicast Routing Forwarding
	ip pim dense-mode	Enable the PIM-DM on interface.
	ip pim sparse-mode	Enable the PIM-SM on the interface

Platform description	None

38.1.9 show ip rpf

This command allows you to show the RPF information of the specific source address.

show ip rpf {*source-address*}

	Parameter	**Description**
Parameter description	*source-address*	Specified source address

Default	None

Command mode	Privileged mode.

Usage guideline	None

Examples	The following example shows the information of the RPF to 192.168.1.54:
	`DGS-3610# 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`

Platform description	None

38.1.10 show ip mvif

Show the basic information of the multicast interface.

show ip rpf { *interface-type interface-number* }

Parameter description

Parameter	Description
interface-type interface-number	Specify an interface

Default	None

Command mode	Privileged mode.

Usage guideline	None

Examples	The following example shows the basic information of the multicast interface of svi1.
	`DGS-3610#`**`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`

Platform description	None

39 Configuring Port-based Flow Control Command

39.1 Configuration Related Commands

Port security module configuration includes the following commands:

- **strom-control**
- **switchport protected**
- **switchport port-security**
- **switchport port-security aging**
- **switchport port-security mac-address**
- **port-security arp-check**

39.1.1 storm-control

Use this command to set the switch of the storm-control of the interface. Use the **no** form of the command to disable the storm-control.

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 control function.
multicast	Enable the unknown miltcast storm control function.
unicast	Enable the unknown unicast storm control function.
percent	Set according to the bandwidth percentage, for example, 20 means 20%
packets	Set according to the **pps**, which means packets per second
Rate-bps	rate allowed

64k-2M	in the unit of measure of 64k
2-100M	in the unit of measure of 1M
About 100M	in the unit of measure of 8M

Default configuration	By default, the storm control function for broadcast, multicast and unicast is disabled.
Command mode	Interface configuration mode.
Usage guidelines	Storm of data packet will occurred when a port receives excessive packets of broadcast,,multicast, or unicast, and may lead to slow network speed or increase overtime. Protocol stack implementation errors or wrong network configuration may also lead to such storms. The device can implement the storm-control to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the device temporarily prohibits forwarding of relevant types of packets till data flows are recovered to the normal state (then packets will be forwarded normally). Use **show storm-control** to view the configuration.

Examples	The following example enables the multicast storm control on GigabitEthernet 1/1 and sets the allowed rate to 4M.
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface GigabitEthernet 1/1`
	`DGS-3610(config-if)# storm-control multicast 4096`
	`DGS-3610(config-if)# end`

Related commands	**Command**	**Description**
	show storm-control	Show storm control information.

39.1.2 switchport protected

Use this command to configure the interface as protected interface. Use the **no** form of the command to disable the protected interface.

switchport protected

no switchport protected

Default configuration	The protected interface is disabled by default.
Command mode	Interface configuration mode.
Usage guidelines	After these interfaces are set as the protected interfaces , between the protected interfaces can not switch on L2, but can route on L3. Switching can be executed between the protected ports. Use **show interfaces** to display configuration.
Examples	DGS-3610(config)#**interface gigabitethernet** 1/1 DGS-3610(config-if)# **switchport protected**

Related commands

Command	Description
show interfaces	Show the interface information.

39.1.3 protected-ports route-deny

L3 route can be executed between the protected ports. This command is disabled the L3 routing between the protected ports.

protected-ports route-deny

no protected-ports route-deny

Default configuration	L3 routing is enabled
Command mode	Global configuration mode.
Usage guidelines	After these ports are set as the protected interfaces, between the protected interfaces can not switch on L2. After configuring this command, the L3 route can be communicationed between the protected interfaces. Use **show running-config** to display configuration.
Examples	DGS-3610(config)# **protected-ports route-deny**

	Command	Description
Related commands	**show running-config**	Check whether L3 block between protection interfaces is enabled

39.1.4 switchport port-security

Use this command to configure port security and its violation. Use the **no** form of the command to disable the port security or restore the violation mode to the default value.

switchport port-security [violation {protect | restrict | shutdown}]

no switchport port-security [violation]

	Parameter	Description
Parameter description	**port-security**	Enable port security
	violation protect	Discards the violated packets while violate
	violation restrict	Discards the violated packets and sends the trap in case of violation.
	violation shutdown	Discards the packets violated and sends the trap and shut down the interface in case of violation.

Default configuration	The security default is disabled.
Command mode	Interface configuration mode.
Usage guidelines	Based on the feature of port security, you can exercise strict control over the input of a specific port by restricting access to the MAC address and IP (optional) of the port on the device. After you configure some secure addresses for the secure port (whose port security function is enabled), this port does not forward any other packets than those whose source addresses are the secure ones. 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 M 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 violation mode is shutdown:

```
DGS-3610(config)#interface gigabitethernet 1/1
DGS-3610(config-if)# switchport port-security
DGS-3610(config-if)# switchport port-security
violation shutdown
```

Related commands

Command	Description
show port-security	Show port security settings for the specified interface.

39.1.5 switchport port-security aging

You can use port security aging to set the aging time for all secure addresses on a port. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the device 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 security aging.

switchport port-security aging {static | time *time* }

no switchport port-security aging {static | time }

Parameter description

Parameter	Description
Static	Denote the aging time for both secure addresses of manually configured and automatically learned. Otherwise it only automatically learned secure addresses.
time *time*	Indicates the aging time for the secure address on this port. Its range is 0-1440 in minute. If you set it to 0, the aging function actually is disabled.

Default configuration Not any security addresses are aged.

Command mode Interface configuration mode.

Usage guidelines	In interface configuration mode, use **no switchport port-security aging time** to disable the port security aging. Use the **no switchport port-security aging static** to apply the aging time only on dynamically learned security address. Use **show port-security** to display configuration.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# switchport port-security aging time 8
DGS-3610(config-if)# switchport port-security aging static
```

Related commands

Command	Description
show port-security	Show port security settings for the specified interface.

39.1.6 switchport port-security mac-address

Use this command to configure the port security address table. Use the **no** form of the command to remove the configuration or restore the default setting.

switchport port-security [**mac-address** *mac-address* [**ip-address** *ip-address*]] | [**maximum** *value*]

no switchport port-security [**mac-address** *mac-address*] | [**maximum**]

Parameter description

Parameter	Description
mac-address *mac-address**s***	Set the secure MAC address of the port
ip-address *ip-address*	IP address bound up with the secure address.
maximum *value*	The maximum number of the addresses in the secure address table.

Default configuration	No any security address
Command mode	Interface configuration mode.

Usage guidelines	This combination statement of IP address and MAC address consumes the hardware resource shared with the applications such as ACLs. So if the device has configured with ACLs or enabled 802.1x authentication feature on a port, and the IP addresses is selected. The numer of configured secure address for stating IP address on this port will be decreased.

Examples

The example below describes how to configure a secure address for interface gigabitethernet 1/1: 00d0.f800.073c and bind it with an IP address:192.168.12.202:

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# switchport mode access
DGS-3610(config-if)# switchport port-security
DGS-3610(config-if)# switchport port-security
mac-address 00d0.f800.073c ip-address 192.168.12.202
```

Related commands

Command	Description
show port-security	Show port security settings and secure address for the specified interface.

39.1.7 Switchport port-security arp-check

Configure the ARP check. You can use the **no** form of the command to disable this function.

[**no] switchport port-security arp-check [cpu]**

Parameter description

Parameter	Description
cpu	check the packets sent to the CPU of the device.

Default configuration	Disabled by default.
Command mode	Interface configuration mode.

Examples

```
DGS-3610(config-if)# switchport port-security arp-check
```

Related commands

Command	Description
show port-security	Show the port-security configuration.

39.2 Showing Related Command

The following commands are used to show the security configuration of the port:

show storm-control

show port-security

show port-security arp-check

39.2.1 show storm-control

Show storm control information.

show storm-control [*interface-id*]

Parameter description

Parameter	Description
interface-id	Configure the storm control on specified interface.

Default configuration All information is displayed.

Command mode Privileged mode.

Examples

```
DGS-3610# show storm-control gigabitethernet 1/1
Interface Broadcast Control Multicast Control Unicast Control
---------- --------------- ---------------- ---------------
Gi1/1 Disabled Disabled Disabled
```

Related commands

Command	Description
storm-control	Use this command to enable the storm-control.

39.2.2 show port-security

Show port security settings for the specified interface.

show port-security [address] [interface *interface-id***]**

Parameter description

Parameter	Description
address	Show all the secure address or the secure address on the specified interface.
interface *interface-id*	Show the port security configuration of the specified interface.

Command mode

Privileged mode.

Usage guidelines

Show all the port security configurations, secure address and the violation processing if no parameter.

Examples

```
DGS-3610# 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	Use this command to configure port security and its violation.
switchport port-security aging	Specify the aging time fpr the secure address on the interface.
switchport port-security mac-address	Use this command to configure the port security address table.

40 Configuring 802.1X Command

40.1 dot1x Active Authentication Command

The dot1x active authentication commands include:

- **dot1x auto-req**
- **dot1x auto-req packet-num**
- **dot1x auto-req req-interval**
- **dot1x auto-req user-detect**

40.1.1 dot1x auto-req

To configure 802.1X active authentication function, execute the global configuration command **dot1x auto-req**. The **no** form of this command is used to disable the automatic authentication function.

[**no**] **dot1x auto-req**

Parameter description	None
Default	Active authentication is not configured.
Command mode	Global configuration mode.
Usage guidelines	To set the device to automatically initiate 802.1x authentication, 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:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x auto-req`
	`DGS-3610(config)# end`
	`DGS-3610# show dot1x auto-req`

```
DGS-3610(config)# dot1x auto-req

Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Second
```

Related commands

Command	Description
show dot1x auto-req	View the active authentication setting information.

40.1.2 dot1x auto-req packet-num

Set the number of authentication request packets 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 packets that the device sends automatically

Default

num = 0; namely the packets are sent continuously

Command mode

Global configuration mode.

Usage guidelines

To set the number of authentication request packets that the device sends automatically, 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:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x auto-req packet-num 0
DGS-3610(config)# end
DGS-3610# show dot1x auto-req

Auto-Req: Enabled
User-Detect : Enabled
```

```
Packet-Num  : 0
Req-Interval: 30 Second
```

Related commands

Command	Description
show dot1x auto-req	View the automatic authentication setting information.

40.1.3 dot1x auto-req req-interval

Set the number of authentication request packets that the device automatically sends. 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 automatically sending authentication request packets by the device, in second

Default

30 seconds

Command mode

Global configuration mode.

Usage guidelines

To set the number of authentication request packets that the device sends automatically, use the **show dot1x auto-req** command to view the setting of this function.

Examples

The following example sets the time interval of device initiating 802.1x authentication to 60s:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x auto-req req-interval 60
DGS-3610(config)# end
DGS-3610# show dot1x auto-req

Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 60 Second
```

	Command	Description
Related commands	**show dot1x auto-req**	View the active authentication setting information.

40.1.4 dot1x auto-req user-detect

Set the number of authentication request packets that the device actively sends. The no form is used to specify the default value.

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter description	This command has no parameters.
Default	Enabled.
Command mode	Global configuration mode.
Usage guidelines	To set the number of authentication request packets that the device sends actively, 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 requests after the user gets on line:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x auto-req user-detect`
	`DGS-3610(config)# end`
	`DGS-3610# show dot1x auto-req`
	
	`Auto-Req: Enabled`
	`User-Detect : Enabled`
	`Packet-Num : 0`
	`Req-Interval: 60 Second`

	Command	Description
Related commands	**show dot1x auto-req**	View the active authentication request information.

40.2 dot1x Timeout Parameter Setting Commands

The dot1x timeout parameter setting commands include:

- **dot1x timeout quiet-period**
- **dot1x timeout re-authperiod**
- **dot1x timeout server-timeout**
- **dot1x timeout supp-timeout**
- **dot1x timeout tx-period**

40.2.1 dot1x timeout quiet-period

Use this command to set the time (in seconds) to wait for the re-authentication attempt after the device fails in authentication (for example, incorrect authentication password). Use the **no** form of the command to restore the default setting.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameter description

Parameter	Description
seconds	Waiting time from failure of device authentication and allowed reattempt of authentication. The range is from 0 to 65535, in seconds.

Default

10 seconds by default.

Command mode

Global configuration mode.

Usage guidelines

When authentication fails, the user is not allowed to reauthenticate immediately, and must be held for some time.The **show dot1x** command can be used.

Examples

The following example sets the time for waiting re-authentication to 1000s:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x timeout quiet-period 1000
DGS-3610(config)# end
DGS-3610# 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	Use this command to display the information about 802.1x.

40.2.2 dot1x timeout re-authperiod

This command sets re-authentication interval when re-authentication is enabled, namely the period of authentication. Use the **no** form of the command to restore 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, in second.

Default

3600 seconds

Command mode

Global configuration mode.

Usage guidelines

Use **show dot1x** command to display 802.1X configuration.

Examples

The following example sets the period of re-authentication to 1000s:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x timeout re-authperiod 1000
DGS-3610(config)# end
```

```
DGS-3610# 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	Use this command to display the information about 802.1x.

40.2.3 dot1x timeout server-timeout

This command sets timeout value of authentication interaction between device and authentication server. Use the **no** form of the command to restore the default setting.

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameter description

Parameter	Description
seconds	Timeout value between device and authentication server for authentication. The range is 0 to 65535 seconds.

Default

5 seconds

Command mode

Global configuration mode.

Usage guidelines

Use **show dot1x** command to display 802.1X configuration.

Examples

The following example sets the timeout value of server interaction to 10s:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x timeout server-timeout 10
DGS-3610(config)# end
DGS-3610# 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	Use this command to display the information about 802.1x.

40.2.4 dot1x timeout supp-timeout

This command sets timeout value of authentication interaction between device and supplicant. Use the **no** form of the command to restore the default setting.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameter description

Parameter	Description
seconds	Timeout value of authentication interaction between device and supplicant. The range is from 0 to 65535 seconds.

Default

3 seconds

Command mode

Global configuration mode.

Usage guidelines	Use **show dot1x** command to display 802.1X configuration.

Examples

The following example sets the timeout value of client interaction to 10s:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x timeout supp-timeout 10
DGS-3610(config)# end
DGS-3610# 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	Use this command to display the information about 802.1x.

40.2.5 dot1x timeout tx-period

This command sets the retransmission time interval after setting the maximam number of packet retransmission, namely the period of retransmission. Use the **no** form of the command to restore 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 by default.
Command mode	Global configuration mode.
Usage guidelines	Use **show dot1x** command to display 802.1X configuration.

Examples	The following example sets the interval of retransmission to 10s:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x timeout tx-period 10`
	`DGS-3610(config)# end`
	`DGS-3610# 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	Use this command to display the information about 802.1x.

40.3 dot1x Re-authentication Commands

Re-authentication commands include:

- **dot1x re-authentication**
- **dot1x reauth-max**

40.3.1 dot1x re-authentication

Use this command to enable periodic re-authentication. Use the **no** form of the command to restore the default setting.

[**no**] **dot1x re-authentication**

Parameter description	This command has no parameters.
Default	By default, the supplicant is not required to re-authenticate at periodical intervals.
Command mode	Global configuration mode.
Usage guidelines	The client has to re-authenticate after specific interval if authentication is passed. Use **show dot1x** command to display 802.1X configuration.

Examples	The following example enables the re-authentication function:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x re-authentication`
	`DGS-3610(config)# end`
	`DGS-3610# 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	Use this command to display the information about 802.1x.

40.3.2 dot1x reauth-max

This command sets maximal re-authentication times. Use the **no** form of the command to restore 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 failures of re-authentication for the supplicant. Use **show dot1x** command to display 802.1X configuration.

Examples

The following example sets the maximum number of re-authentications:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x reauth-max 5
DGS-3610(config)# end
DGS-3610# 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

Command	Description

commands	**show dot1x**	Use this command to display the information about 802.1x.

40.4 dot1x Detection Function Commands

The detection function commands include:

- **dot1x probe-timer**
- **dot1x client-probe enable**

40.4.1 dot1x probe-timer

Use this command to configure client probing timer parameters.

dot1x probe-timer{**interval** | **alive**}*interval*

no dot1x probe-timer

Parameter description

Parameter	Description
no	Restores the default value
interval	hello interval
alive	Alive interval
interval	Timer value

Default

The default Hello interval is 20 seconds.
Default online 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 view the 802.1x setting.

Examples

The following example sets the hello interval to 30 seconds and the alive interval to 120 seconds:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x probe-timer interval 30
DGS-3610(config)# dot1x probe-timer alive 120
DGS-3610(config)# end
DGS-3610# show dot1x probe-timer

Hello Interval: 30 Seconds
```

```
Hello Alive: 120 Seconds
```

Related commands	Command	Description
	Show dot1x probe-timer	Show client probing configurations.

40.4.2 dot1x client-probe enable

Enable the on-line probe function of the client

[**no**] **dot1x client-probe enable**

Parameter description	No parameters.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Use this command to set the on-line probe function of the client
Examples	Enable the on-line probe function of the client

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x client-probe enable
DGS-3610(config)# end
DGS-3610# 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 dot1x configurations.

40.5 Other dot1x Configuration Commands

Other dot1x configuration commands include:

- **dot1x authentication**
- **dot1x auth-address-table**
- **dot1x auth-mode**
- **dot1x default**
- **dot1x dynamic-vlan enable**
- **dot1x eapol-tag**
- **dot1x max-req**
- **dot1x private-supplicant-only**
- **dot1x port-control auto**
- **dot1x port-control-mode**
- **dot1x stationarity enable**

40.5.1 dot1x authentication

In case the AAA is enabled, the authentication with the AAA server must be performed for logon. This command is used 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.

```
DGS-3610# configure terminal
DGS-3610(config)# aaa new-model
DGS-3610(config)# aaa authentication dot1x default group radius
DGS-3610(config)# interface fastEthernet0/1
DGS-3610(config-if)# dot1x authentication default
DGS-3610(config-if)# end
DGS-3610#
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service
aaa authentication dot1x	Configure the logon authentication method list

40.5.2 dot1x auth-address-table

This command configures 802.1X authentication-allowed address list. Use the **no** form of the command to remove the authentication-allowed address.

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 address that can be authenticated.
interface	Interface number.

Default

No authenticated address by default.

Command mode

Global configuration mode.

Usage guidelines

Only the address in this list can be authenticated 802.1X. Use **show dot1x auth-address table** command to display the authentication address list.

Examples

The following example demonstrates how to add an authentication

address on the interface.

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x auth-address-table address
00d0f8000000 interface ehternet 1/1
DGS-3610(config)# end
DGS-3610#
```

Related commands

Command	Description
show dot1x auth-address-table	Show 802.1X authentication-allowed address list

40.5.3 dot1x auth-mode

Specify the 802.1x authentication mode.

dot1x auth-mode {**eap-md5** | **chap** | **pap**}

no dot1x auth-mode

Parameter description

Parameter	Description
eap-md5	802.1x uses EAP-MD5 authentication mode
chap	802.1x uses CHAP authentication mode
pap	802.1x uses PAP authentication mode

Default

EAP-MD5 mode

Command mode

Global configuration mode.

Usage guidelines

Use the **show dot1x** command to display 802.1X configurations.

Examples

This example shows how to configure 802.1X authentication mode:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x auth-mode chap
DGS-3610(config)# end
DGS-3610#
```

Related commands

Command	Description
show dot1x	Use this command to display the information about 802.1x.

40.5.4 dot1x default

Restore the parameters in the 802.1x setting part in the device to the default values.

dot1x default

Parameter description	This command has no parameters.
Default	None
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x** command to display 802.1X configuration.

Examples	The following example sets the default parameters of 802.1x:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x default`
	`DGS-3610(config)# end`
	`DGS-3610# end`

Related commands

Command	Description
show dot1x	Use this command to display the information about 802.1x.

40.5.5 dot1x dynamic-vlan enable

Configure whether to allow dynamic vlan jumping. You can use the **no** form of the command to turn off this switch.

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameter description	This command has no parameters.
Default	This switch is disabled by default.
Command mode	Global configuration mode.

Usage guidelines	Use the **show dot1x dynamic-vlan** command to display 802.1X configuration.

Examples	The following example shows how to sets dynamic vlan jumping of 802.1x:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x dynamic-vlan enable`
	`DGS-3610(config)# end`
	`DGS-3610#`

Related commands	**Command**	**Description**
	show dot1x	Use this command to display the information about 802.1x.

40.5.6 dot1x eapol-tag

Enable the flag for EAPOL frames with the function of TAG.

dot1x eapol-tag

no dot1x eapol-tag

Parameter description	This command has no parameters.
Default	This switch is disabled by default.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x** command to display 802.1X configuration.

Examples	The following example shows how to allow the 802.1X frame to have a tag:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x eapol-tag`
	`DGS-3610(config)# end`
	`DGS-3610#`

Related commands

Command	Description
show dot1x	Use this command to display the information about 802.1x.

40.5.7 dot1x max-req

During interaction between DOT1X and the server, 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 the maximum number of requests sent to the server. Use the **no** form of the command to restore the default value.

dot1x max-req *count*

no dot1x max-req

Parameter description

Parameter	Description
count	Maximum number of allowed authentication requests.

Default

The default value is 3.

Command mode

Global configuration mode.

Usage guidelines

Use the **show dot1x** command to display 802.1X configuration.

Examples

The following example demonstrates how to set the maximum number of retransmissions for 802.1x authentication to 7:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x max-req 7
DGS-3610(config)# end
DGS-3610#
```

Related commands

Command	Description
show dot1x	Use this command to display the information about 802.1x.

40.5.8 dot1x private-supplicant-only

This command sets whether to support private client in the global configuration mode. The no form of this command can recover the setting to the default value.

dot1x private-supplicant-only

no dot1x private-supplicant-only

Parameter description	There is no parameter in this command.
Default configuration	The default is not allowed to be filtered.
Command mode	Global configuration mode.
Usage guidelines	You can use **show dot1x private-supplicant-only** to view the 802.1x setting.

Examples	The following example is to allow private clients only:
	`DGS-3610# configure t`
	`DGS-3610(config)# dot1x private-supplicant-only`
	`DGS-3610(config)# end`
	`DGS-3610#`

Related commands

Command	Function
show dot1x private-supplicant-only	View the setting information

40.5.9 dot1x port-control auto

In the interface configuration mode, use this command to set whether the interface participates in authentication. Use the **no** form of the command to restore the default value.

dot1x port-control auto

no dot1x port-control

Parameter description	This command has no parameters.
Default	By default, the interface does not participate in 802.1x authentication.

Command mode	Interface configuration mode.
Usage guidelines	Use the **show dot1x** command to display 802.1X configuration.

Examples	The following example sets the port 802.1x to participate in authentication:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# interface g0/1`
	`DGS-3610(config-if)# dot1x port-control auto`
	`DGS-3610(config-if)# end`
	`DGS-3610#`

Related commands

Command	Description
show dot1x	Use this command to display the information about 802.1x.

40.5.10 dot1x port-control-mode

By default, 802.1x controls users based on user MAC. Only authenticated users 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 a port passes the authentication, this port becomes an authenticated port, and all the users that connect to this port can access to the network. The authentication mode can be configured using the following commands:

dot1x port-control-mode {**mac-based** | **port-based**}

no dot1x port-control-mode

Parameter description

Parameter	Description
mac-based	mac-based 802.1X access control
port-based	port-based 802.1X access control

Default	mac-based access control is used by default.
Command mode	Interface configuration mode.
Usage	Use the **show dot1x port-control** command to display 802.1X

guidelines	configuration for the port. On the S26, the port-based 802.1X and security channel cannot apply to the same port. If the security channel is configured in the global mode, the port with the port-based 802.1X can be set to the exceptional port of the security channel.

Examples

The following example sets the port 802.1x to participate in authentication:

```
DGS-3610(config)# interface g0/1
DGS-3610(config-if)# dot1x port-control auto
DGS-3610(config-if)# dot1x port-control-mode
port-based
DGS-3610(config-if)# end
DGS-3610#
```

Related commands

Command	Description
show dot1x port-control	Display the information about 802.1x setting for the port.

40.5.11 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 transiting from 802.1X port to other ports, you can use the following commands:

dot1x stationarity enable

no dot1x stationarity enable

Parameter description	None
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	Following example is to set the 802.1X port for authentication:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# dot1x stationarity enable`
	`DGS-3610(config)# end`
	`DGS-3610#`

Related commands	None

40.6 dot1x Showing Commands

- **show dot1x**
- **show dot1x auth-address-table**
- **show dot1x auto-req**
- **show dot1x private-supplicant-only**
- **show dot1x max-req**
- **show dot1x port-control**
- **show dot1x probe-timer**
- **show dot1x re-authentication**
- **show dot1x reauth-max**
- **show dot1x summary**
- **show dot1x timeout**
- **show dot1x user id**

40.6.1 show dot1x

Use this command to display the information about 802.1x setting.

show dot1x

Parameter description	This command has no parameters.

Default	None

Command mode	Privileged mode.

Usage guidelines

None

Examples

```
See the following example:
DGS-3610# 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
DGS-3610#
```

Related commands

Command	Description
dot1x auth-mode	Specify the 802.1x authentication mode.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.

	dot1x timeout tx-period	Specify the retransmission period

40.6.2 show dot1x auth-address-table

Use this command to display 802.1X authentication-allowed address table.

show dot1x auth-address-table[*addressmac-addr*][*interface interface*]

Parameter description

Parameter	Description
mac-addr	Physical address that can be authenticated.
interface	Interface number.

Default

None

Command mode

Privileged mode.

Usage guidelines

None

Examples

See the following example:

```
DGS-3610# show dot1x auth-address-table
interface:g3/1
---------------------------------
mac-addr 00D0.F800.0001
DGS-3610#
```

Related commands

Command	Description
dot1x auth-mode	Specify the 802.1x authentication mode.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute.
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.

	dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
	dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
	dot1x timeout tx-period	Specify the retransmission period

40.6.3 show dot1x auto-req

Show the configuration information of device's automatic initiation of 802.1x authentication.

show dot1x auto-req

Parameter description	No parameters.
Default	None
Command mode	Privileged mode.
Usage guidelines	None

Examples	See the following example:
	`DGS-3610# show dot1x auto-req`
	
	`Auto-Req: Disabled`
	`User-Detect : Enabled`
	`Packet-Num : 0`
	`Req-Interval: 30 Seconds`
	`DGS-3610#`

Related commands	**Command**	**Description**
	dot1x auth-mode	Specify the 802.1x authentication mode.
	dot1x max-req	Specify the maximum retransmission time.
	dot1x port-control auto	Specify whether the interface can take part in authentication

	dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
	dot1x re-authentication	Specify the re-authentication attribute
	dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
	dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
	dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
	dot1x timeout tx-period	Specify the retransmission period

40.6.4 show dot1x private-supplicant-only

Show the client filtering function of the device.

show dot1x private-supplicant-only

Parameter description	No parameters.
Default	None
Command mode	Privileged mode.
Usage guidelines	None

Examples	See the following example:
	`DGS-3610# show dot1x private-supplicant-only`
	`private-supplicant-only:: disabled`
	`DGS-3610#`

Related	**Command**	**Description**

commands	**dot1x auth-mode**	Specify the 802.1x authentication mode.
	dot1x max-req	Specify the maximum retransmission time.
	dot1x port-control auto	Specify whether the interface can take part in authentication.
	dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
	dot1x re-authentication	Specify the re-authentication attribute.
	dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
	dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
	dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
	dot1x timeout tx-period	Specify the retransmission period

40.6.5 show dot1x max-req

Show the maximum number of retransmissions to the client.

show dot1x max-req

Parameter description	No parameters.
Default	None
Command mode	Privileged mode.
Usage guidelines	None
Examples	See the following example:

```
DGS-3610# show dot1x max-req
max-req: 2 times
DGS-3610#
```

Related commands

Command	Description
dot1x auth-mode	Specify the 802.1x authentication mode.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
dot1x timeout tx-period	Specify the retransmission period

40.6.6 show dot1x port-control

Show the ports that participate in authentication.

show dot1x port-control [**interface** *interface*]

Parameter description

Parameter	Description
interface	Specified interface.

Default None

Command mode Privileged mode.

Usage guidelines	None

Examples

See the following example:

```
DGS-3610# show dot1x port-control
interface dyn-user static-user max-user qos     ctrl-mode status
--------- -------- ----------- -------- ------- --------  ------
Gi0/1    0        1           6000     dscp: 0 mac-base Authed
DGS-3610#
```

Related commands

Command	Description
dot1x auth-mode	Specify the 802.1x authentication mode.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
dot1x timeout tx-period	Specify the retransmission period

40.6.7 show dot1x probe-timer

Show client online probing configurations.

show dot1x probe-timer

Parameter description	None

Default	None
Command mode	Privileged mode.
Usage guidelines	Show client probing configurations.

Examples	See the following example:
	`DGS-3610# show dot1x probe-timer`
	
	`Hello Interval: 20 Seconds`
	`Hello Alive: 250 Seconds`
	`DGS-3610#`

Related commands

Command	Description
dot1x auth-mode	Specify the authentication mode of 802.1x.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication.
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
dot1x timeout tx-period	Specify the retransmission period

40.6.8 show dot1x re-authentication

Show re-authentication configuration.

show dot1x re-authentication

Parameter description	None
Default	None
Command mode	Privileged mode
Usage guidelines	Re-authentication configuration.

Examples	See the following example:
	`DGS-3610# show dot1x re-authentication`
	`eauth-enabled: disabled`
	`DGS-3610#`

Related commands

Command	Description
dot1x auth-mode	Specify the authentication mode of 802.1x.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
dot1x timeout	Set the timeout value of authentication

	supp-timeout	interaction between device and supplicant.
	dot1x timeout tx-period	Specify the retransmission period

40.6.9 show dot1x reauth-max

Show the maximum number of re-authentications.

show dot1x reauth-max

Parameter description	None
Default	None
Command mode	Privileged mode.
Usage guidelines	Show the specified times of re-authentications.

Examples	See the following example:
	`DGS-3610# show dot1x reauth-max`
	`reauth-max: 2 times`
	`DGS-3610#`

Related commands

Command	Description
dot1x auth-mode	Specify the 802.1x authentication mode.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.

	dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
	dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
	dot1x timeout tx-period	Specify the retransmission period

40.6.10 show dot1x summary

Use this command to display 802.1X authentication configuration summary.

show dot1x summary

Parameter description	None
Default	None
Command mode	Privileged mode.
Usage guidelines	Show configuration summary.

Examples	See the following example:
	`DGS-3610# show dot1x summary`
	`ID MAC Interface VLAN Auth-State Backend-State Port-Status Type`
	`- -------- ---------- ----------- ------------- ---------- -----`
	`1 00d0f8000000 Gi0/1 1 Authenticated Idle Authed Static`
	`DGS-3610#`

Related commands	**Command**	**Description**
	dot1x auth-mode	Specify the 802.1x authentication mode.
	dot1x max-req	Specify the maximum retransmission time.
	dot1x port-control auto	Specify whether the interface can take part in authentication
	dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.

	dot1x re-authentication	Specify the re-authentication attribute
	dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
	dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
	dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
	dot1x timeout tx-period	Specify the retransmission period

40.6.11 show dot1x user id

Use this command to display 802.1X authentication summary.

show dot1x user id <*id*>

Parameter description	**Parameter**	**Description**
	id	User id in show summary

Default	None
Command mode	Privileged mode.
Usage guidelines	Show information about a specific user.

Examples	See the following example:
	`DGS-3610# 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

DGS-3610#
```

Related commands

Command	Description
dot1x auth-mode	Specify the 802.1x authentication mode.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the timeout value of authentication interaction between device and authentication server.
dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
dot1x timeout tx-period	Specify the retransmission period

40.6.12 show dot1x timeout

The command shows information about the 802.1X timeout parameter.

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	None
Default	None
Command mode	Privileged mode.
Usage guidelines	Show configuration of the timeout parameter.

Examples	See the following example:
	`DGS-3610# show dot1x timeout quiet-period`
	`quiet-period: 60 sec`
	`DGS-3610#`

Related commands

Command	Description
dot1x auth-mode	Specify the 802.1x authentication mode.
dot1x max-req	Specify the maximum retransmission time.
dot1x port-control auto	Specify whether the interface can take part in authentication
dot1x reauth-max	Specify the maximum re-authentication time of the supplicant.
dot1x re-authentication	Specify the re-authentication attribute
dot1x timeout quiet-period	Specify the waiting time from failure of device authentication and allowed reattempt of authentication.
dot1x timeout re-authperiod	Specify the re-authentication period for the supplicant.
dot1x timeout	Set the timeout value of authentication

	server-timeout	interaction between device and authentication server.
	dot1x timeout supp-timeout	Set the timeout value of authentication interaction between device and supplicant.
	dot1x timeout tx-period	Specify the retransmission period

41 Configuring AAA Command

41.1 ID Authentication Related Command

- **aaa authentication**

41.1.1 aaa authentication

To use AAA for user authentication, execute the global configuration command **aaa authentication** to configure the user authentication method list. The **no** form of this command is used to delete the user authentication method list.

aaa authentication {**dot1x** | **enable** | **ppp** | **login**} {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication {**dot1x** | **enable** | **ppp** | **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 user authentication.
list-name	Define a method list for login authentication. It can be any string.
dot1x	Dot1x user
enable	Enable user
ppp	PPP user
login	Login user
method	It must be one of the keywords listed in the follwing table. One method list can contain up to four methods.

Table 41-1 AAA user authentication methods

Keyword	Description
local	Use the local user name database for ID authentication
none	Do not perform ID authentication

		group	Use the server group for id authentication. At present, the RADIUS server group is supported

Default

If no **default** method list is configured, the following method is used:
aaa authentication {**dot1x** | **enable** | **ppp** | **login**} **default group radius**

Command mode

Global configuration mode.

Usage guidelines

If the AAA security service is enabled in the device, users must use AAA for authentication negotiation. You must use **aaa authentication** to configure a default or optional method list for 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.

```
DGS-3610(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 on the DOT1x interface
ppp authentication	PPP association specific method list
login authentication	Login association specific method list
username	Defines a local user database

41.2 Authorization Related Commands

At present, DGS-3610 SERIES supports authorization to the network protocols, including the following related commands:

- **aaa authorization network**

41.2.1 aaa authorization network

To use AAA to authorize the service requests (including such protocols as PPP and SLIP) from users that access the network, execute the global configuration command **aaa authorization network**. The **no** form of this command is used to disable the AAA authorization function.

aaa authorization network {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization network {**default** | *list-name*}

Parameter description

Parameter	Description
method1	It must be one of the keywords listed in the following table:

Keyword	Description
local	Use the local user name database for network authorization
none	Do not perform network authorization
group	Use the server group for authentication. At present, the RADIUS server group is supported

Default

The AAA authorization function is disabled.

Command mode

Global configuration mode.

Usage guidelines

DGS-3610 SERIES 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 authentication, 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 authentication. RADIUS authorization is performed only when the user passes the RADIUS authentication.

Examples

The following example uses the RADIUS server to authorize network services:

```
DGS-3610(config)# aaa authorization network default radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service
aaa accounting	Define AAA accounting
aaa authentication	Define AAA authentication
Username	Defines a local user database

41.3 Accounting Related commands

At present, DGS-3610 SERIES supports network accounting using RADIUS, including the following related commands:

- **aaa accounting network**
- **aaa accounting update**
- **aaa accounting update periodic**
- **show aaa method-list**
- **debug aaa**

41.3.1 aaa accounting network

To perform accounting of access activities of users in order to count the network access fees or manage user activities, execute the global configuration command **aaa accounting network**. 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 accounting method list.
start-stop	Accounting messages are sent at both the start and end of user access activities. 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

The accounting function is disabled.

Command mode

Global configuration mode.

Usage guidelines

DGS-3610 SERIES 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 accounting messages at the start and end:

```
DGS-3610(config)# aaa accounting network start-stop group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service
aaa authorization network	Define AAA network authorization
aaa authentication	Define AAA authentication
username	Defines a local user database

41.3.2 aaa accounting update

To enable the accounting update function, execute the global configuration command **aaa accounting update**. This command is used to enable the global accounting update. The **no** form of this command is used to disable the accounting update function.

aaa accounting update

no aaa accounting update

Parameter description	No parameters.
Default	The accounting update function is disabled by default.
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.
	`DGS-3610(config)# aaa new-model`
	`DGS-3610(config)#`

Related commands

Command	Description
aaa new-model	Enable the AAA security service
aaa accounting network	Define a network accounting method list

41.3.3 aaa accounting update periodic

If the accounting update function has been enabled, execute the global configuration command **aaa accounting update periodic**. This command is used to set the interval of accounting update. The **no** form of this command is used to configure the default interval of accounting update.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter description

Parameter	Description
interval	Interval of accounting update, 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.

```
DGS-3610(config)# aaa new-model
DGS-3610(config)# aaa accounting update
DGS-3610(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

41.3.4 show aaa method-list

To view all the current user method lists, execute the privilege EXEC command **show aaa methold-list**.

show aaa method-list

Command mode No keyword and parameter.

Command mode Privileged EXEC configuration mode.

Examples DGS-3610# **show aaa method-list**

41.4 AAA Server Group Commands

- **show aaa group**
- **aaa group server**
- **server ip-addr authen-port port1 acct-port port2**
- **ip vrf forwarding**

41.4.1 show aaa group

Show all the server groups configured for AAA.

show aaa group

Parameter description	No parameter or keyword for the command
Default	None
Command mode	Privileged mode.
Usage guidelines	This command shows all the server groups configured for AAA.

Examples	See the following example.
	`DGS-3610# 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`
	`DGS-3610#`

Related commands

Command	Description
aaa group server	Configure the AAA server group

41.4.2 aaa group server

Enter the AAA server group configuration mode. The **no** form of this command is used to delete the server group.

aaa group server radius *name*

no aaa group server radius *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 server group is supported.

Examples

See the following example.

```
DGS-3610(config)# aaa group server radius ss
DGS-3610(config-gs-radius)# end
DGS-3610# show aaa group
Group-name:  ss
Group Type:  radius
Referred:    1
Server List:
DGS-3610#
```

Related commands

Command	Description
show aaa group	Show the AAA server group

41.4.3 server *ip-addr* authen-port *port1* acct-port *port2*

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	See the following example.
	`DGS-3610(config)# aaa group server radius ss`
	`DGS-3610(config-gs-radius)# server 192.168.4.12 acct-port 5 authen-port 6`
	`DGS-3610(config-gs-radius)# end`
	`DGS-3610# 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`
	`DGS-3610#`

Related commands

Command	Description
aaa group server	Configure the AAA server group
show aaa group	Show the AAA server group

41.4.4 ip vrf forwarding

This command selects the vrf for the AAA server group. The "no" form of this command can delete the selection.

ip vrf forwarding vrf_name

no ip vrf forwarding

Parameter description

Parameter	Description
vrf_name	The **vrf_name** is the name of vrf .

Default	None
Command mode	Server group configuration mode.
Usage guidelines	This command selects vrf for specified server groups.

Examples	The following is an example.
	`DGS-3610(config)# aaa group server radius ss`
	`DGS-3610(config-gs-radius)# server 192.168.4.12`
	`DGS-3610(config-gs-radius)# server 192.168.4.13`
	`DGS-3610(config-gs-radius)# ip vrf forwarding vrf_name`
	`DGS-3610(config-gs-radius)# end`
	`DGS-3610#`

Related commands

Command	Description
aaa group server	Configure the AAA server group
show aaa group	Show the AAA server group

41.5 Other AAA Commands

- **aaa new-model**
- **debug aaa**
- **show aaa method-list**

41.5.1 aaa new-model

To use the AAA security service function of DGS-3610 SERIES, execute the global configuration command **aaa new-model** to enable AAA. The **no** form of this command is used to disable the AAA security service.

aaa new-model

no aaa new-model

Parameter description	No parameter or keyword for the command
Default	The AAA security service is disabled.

Command mode	Global configuration mode.
Usage guidelines	This command is used to enable AAA. To use the AAA security service, you must enable the AAA security service using **aaa new-model**. 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. `DGS-3610(config)# aaa new-model`

Related commands

Command	Description
aaa authentication	Defines a user authentication method list

41.5.2 debug aaa

It is used to turn on the AAA service debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug aaa

no debug aaa

Parameter description	No parameter or keyword.
Command mode	Privileged EXEC configuration mode.

41.5.3 show aaa method-list

Show all the method lists for AAA.

show aaa method-list

Parameter description	No parameter or keyword for the command
Default	None

Command mode

Privileged mode

Usage guidelines

This command shows all the method lists for AAA.

Examples

The following example sows the AAA method list.

```
DGS-3610# 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
DGS-3610#
```

Related commands

Command	Description
aaa authentication	Defines a user authentication method list
aaa authorization	Defines a user authorization method list
aaa accounting	Defines a user accounting method list

42 Configuring RADIUS Command

42.1 RADIUS Configure related command

RADIUS configuration includes following commands:

- **ip raius source-interface**
- **radius-server host**
- **radius-server key**
- **radius-server retransmit**
- **radius-server timeout**
- **radius-server dead-time**
- **radius attribute**
- **radius set qos cos**
- **radius vendor-specific extend**

42.1.1 ip radius source-interface

To specify the source address for the radius packet, execute the global configuration command **ip radius source-interface**. Use the **no** form of this command to delete the source address for a specified RADIUS packet.

ip radius source-interface *interface*

no radius source-interface

Parameter description	**Parameter**	**Description**
	Interface	Interface at the source address of the RADIUS packet

Default	The source 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 address of the RADIUS packet. This command uses the first IP address of the specified interface as the source 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 address of the RADIUS packet: `DGS-3610(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

42.1.2 radius-server host

To specify a RADIUS security server host, execute the global configuration command radius-server. The **no** form of this command is used to delete a specified RADIUS security server host.

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

no radius-server host {*hostname* | *ip-address*}

Parameter description

Parameter	Description
hostname	The DNS name of the RADIUS security server host.
Ip-address	The IP address of the RADIUS security server host.
Auth-port	The UDP port for RADIUS authentication.
*Port-numbe*r	Number of the UDP port for RADIUS authentication. If it is set to 0, this host does not perform ID authentication.
Acct-port	The UDP port for RADIUS accounting.

	Port-number	Number of the UDP port for RADIUS accounting. If it is set to 0, this host does not perform accounting.

Default No RADIUS host is specified.

Command mode Global configuration mode.

Usage guidelines In order to implement the AAA security service by using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server** command.

Examples The following example defines a RADIUS security server host:

```
DGS-3610(config)# radius-server host 192.168.12.1
```

Related commands

Command	Description
aaa authentication	Define 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 timer for the RADIUS packet.

42.1.3 radius-server key

To define a shared password to be used for the network access server (router) to communicate with the RADIUS security server, execute the global configuration command radius-server key. The **no** form of this command is used to cancel the specified shared password.

radius-server key *text-string*

no radius-server key

Parameter description

Parameter	Description
text-string	Text of the shared password

Default	No shared password is specified.
Command mode	Global configuration mode.
Usage guidelines	Shared password is the basis for correct communication 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: `DGS-3610(config)# radius-server key aaa`

Related commands

Command	Description
radius-server host	Define the host of the RADIUS security server
radius-server retransmit	Define the number of RADIUS packet retransmissions
radius-server timeout	Define the timeout timer for the RADIUS packet.

42.1.4 radius-server retransmit

To configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond, execute the global configuration command radius-server retransmit. The **no** form of this command is used to restore the default number of retransmissions.

radius-server retransmit *retries*

no radius-server retransmit

Parameter description

Parameter	Description
retries	Number of RADIUS transmission retries

Default	The default number of transmission retries 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. If the security server does not respond each time when the device retransmits the RADIUS packet for 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: `DGS-3610(config)# radius-server retransmit 4`

Related commands

Command	Description
radius-server host	Define the host of the RADIUS security server
radius-server key	Define a shared password for RADIUS server
radius-server timeout	Define the timeout timer for the RADIUS packet.

42.1.5 radius-server timeout

To set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet, use the global configuration command **radius-server timeout**. The **no** format of this command is used to restore default.

radius-server timeout *seconds*

no radius-server timeout

Parameter description

Parameter	Description
seconds	Timeout, in seconds. The value range is 1-1000 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: `DGS-3610(config)# radius-server timeout 10`

Related commands

Command	Description
radius-server host	Define the host of the RADIUS security server
radius-server retransmit	Define the number of RADIUS packet retransmissions
radius-server key	Define a shared password for RADIUS server

42.1.6 radius-server deadtime

If there is no response within the time **t** after the user sends a packet, the server is considered dead. The time **t** is called deadtime. DGS-3610 series operating system allows you to set the RADIUS deadtime by using the global configuration command **radius-server deadtime**. The **no** format of this command is used to restore default.

radius-server deadtime *minnutes*

no radius-server deadtime

Parameter description

Parameter	Description
minutes	Deadtime (in minutes). The value range is 1-1000 seconds.

Default	5 Minutes
Command mode	Global configuration mode.
Usage guidelines	Use this command to change the timeout of packet retransmission.
Examples	The following example sets the deadtime to 10 minutes: `DGS-3610(config)# radius-server deadtime 10`

Related

Command	Description

commands	**radius-server host**	Define the host of the RADIUS security server
	radius-server retransmit	Define the number of RADIUS packet retransmissions
	radius-server key	Define a shared password for RADIUS server
	radius-server timeout	Define the RADIUS server timeout

42.1.7 radius attribute

radius ttribute{**<***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 <1-255>
type	Private attribute type

Default

Only the default configuration of private attributes in DGS-3610 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-diractory	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 privilige	22
23	login privilige	42

Extension

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-diractory	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 privilige	22

23	login privilige	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 max up-rate type value to 211:

```
DGS-3610(config)# radius attribute 16 vendor-type 211
```

Related commands

Command	Description
radius set qos cos	Defines that the qos value sent by the RADIUS server is the cos value of the interface

42.1.8 radius set qos cos

Defines that the qos value sent by the RADIUS server is used as the cos value of the interface

radius set qos cos

no radius set qos cos

Parameter description None

Default Configure qos as the dscp value.

Command mode Global configuration mode.

Usage guidelines Execute this command to use the sent qos value as the cos value. By default, it is used as the dscp value.

Examples See the following example:

```
DGS-3610(config)# radius set qos cos
```

	Command	Description
Related commands	**radius vendor-specific extend**	Radius is extended to not differentiate private vendor id.

42.2 RADIUS privilege commands

- **debug radius [event | detail]**
- **show radius-server**
- **show radius parameter**
- **show radius vendor-specific**

42.2.1 debug radius

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	No parameter or keyword.

Command mode	Privileged EXEC configuration mode.

42.2.2 show radius server

Show the configuration of the RADIUS server.

show radius server

Parameter description	None

Default	None

Command mode	Privileged EXEC mode

Usage guidelines	Use this command to show the configuration of the RADIUS server.

Examples

```
DGS-3610# show radius server
server ip : 192.168.4.12
acct  port: 23
authen  port: 77
server state: ready
server ip : 192.168.4.13
acct  port: 45
authen  port: 74
server state: ready
```

Related commands

Command	Description
radius-server host	Define the host of the RADIUS security server
radius-server retransmit	Define the number of RADIUS packet retransmissions
radius-server key	Define a shared password for RADIUS server
radius-server timeout	Define the RADIUS server timeout

42.2.3 show radius parameter

Show the global parameters of the RADIUS server.

show radius parameter

Parameter description None

Default None

Command mode Privileged mode.

Usage guidelines Use this command to show the parameters of the RADIUS server.

Examples

```
DGS-3610# show radius parameter
Server Timout:    5 Seconds
Server Deadtime:  5 Minutes
Server Retries:   3
```

```
Server Key:       ******
```

Related commands

Command	Description
radius-server host	Define the host of the RADIUS security server
radius-server retransmit	Define the number of RADIUS packet retransmissions
radius-server key	Define a shared password for RADIUS server
radius-server timeout	Define the RADIUS server timeout

42.2.4 show radius vendor-specific

Show the configuration of the RADIUS private attribute type.

show radius vendor-specific

Parameter description

None

Default

None

Command mode

Privileged mode.

Usage guidelines

Use this command to show the configuration of the RADIUS private attribute type.

Examples

```
DGS-3610# show radius vendor-specific
id    vendor-specific       type-value
----- -------------------- ----------
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-diractory        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 privilige          22
23   login privilige       42
24   limit to user number  50
```

Related commands

Command	Description
radius-server host	Define the host of the RADIUS security server
radius-server retransmit	Define the number of RADIUS packet retransmissions
radius-server key	Define a shared password for RADIUS server
radius-server timeout	Define the RADIUS server timeout

43 Configuring SSH Command

43.1 Configuration Related Commands

SSH configuration includes following commands:

- **crypto key generate**
- **crypto key zeroize**
- **ip ssh version**
- **ip ssh time-out**
- **ip ssh authentication-retries**
- **transport input**

43.1.1 crypto key generate

In global configuration mode, execute following command to generate a public key:

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

Parameter description

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

Default configuration

By default, SSH Server does not generate a public key.

Command mode

Global configuration mode.

Usage guidelines

When you need to enable the SSH Server service, generate a public key for the SSH server using this command to enable the SSH Server service on this device. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if an 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, instead of **no crypto key generate** that is not available.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# crypto key generate rsa
```

Related commands

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

Version description

The software version must be later than v10.1.

43.1.2 crypto key zeroize

Delete the public key , execute following command in global configuration mode:.

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

Parameter description

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

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

This command deletes the public key of the server. After the key is deleted, the SSH Server state becomes DISABLE. If you want to disable the SSH Server, run **no enable service ssh-server**.

Examples

```
DGS-3610# configure terminal
DGS-3610(config)# crypto key zeroize rsa
```

Related commands

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

Version description

The software version must be later than v10.1.

43.1.3 ip ssh version

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

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

no ip ssh version

Parameter description

Parameter	Description
1	Configure SSH Server to only support client connection requests from SSH1
2	Configure SSH Server to only support client connection requests from SSH2

Default configuration

SSH versions 1 and 2 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 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, SSH Server supports SSH1 and SSH2. Clients that use either SSH 1 or SSH 2 can connect to the server. If Version 1 or 2 is set, only the SSH client of this version can connect to the server. Use the **show ip ssh** command to view the current status of SSH Server.

Examples

Only use version 2:

```
DGS-3610# configure terminal
DGS-3610(config)# ip ssh version 2
```

Related commands

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

Version description

The software version must be later than v10.1.

43.1.4 ip ssh time-out

Set the timeout value of user authentication for SSH Server. Use the **no** form of this command to restore the timeout value of user authentication to the default setting.

ip ssh time-out *time*

no ip ssh time-out

Parameter description

Parameter	Description
time	Set the timeout value of user authentication.

Default configuration

The timeout value is 120s by default. After the timeout value is set, restore the setting to the default value using the **no ip ssh time-out** command.

Command mode

Global configuration mode.

Usage guidelines

This command sets the timeout value of user authentication by SSH Server. The authentication is considered timeout and failed if the authentication is not successful within 120s starting from acceptance of user connection request. Use the **show ip ssh** command to view the configuration of SSH server.

Examples

Set the timeout value to 100s:

```
DGS-3610# configure terminal
DGS-3610(config)# ip ssh time-out 100
```

Related commands

Command	Description
show ip ssh	Show the current status of ssh-server.

Version description	The software version must be later than v10.1.

43.1.5 ip ssh authentication-retries

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

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter description

Parameter	Description
retry times	Set the retry times of user authentication.

Default configuration	The default authentication retry times is 3. After the authentication retry times is set, the **no ip ssh authentication-retries** command can be used to restore the setting to the default value.
Command mode	Global configuration mode.
Usage guidelines	This command sets the retry times of user authentication by SSH Server. User authentication is considered failed if authentication is not successful when the configured authentication retry times on SSH Server is exceeded. Use the **show ip ssh** command to view the configuration of SSH Server.

Examples	Set the retry times of user authentication to 2:
	`DGS-3610# configure terminal`
	`DGS-3610(config)# ip ssh ssh authentication-retries 2`

Related commands

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

Version description	The software version must be later than v10.1.

43.2 SSH Showing and Monitoring Commands

The SSH Server showing and monitoring commands include:

- **show ip ssh**
- **show ssh**
- **show crypto key mypubkey**
- **disconnect ssh**

43.2.1 show ip ssh

Show the currently effective configuration information of SSH Server.

show ip ssh

Parameter description	None
Default configuration	None
Command mode	Privilege mode.
Usage guidelines	Show the currently effective configuration information of SSH Server, including version, SSH Server enabled or not, timeout value, and authentication retry times. Note: If no key for the server is generated, the SSH version is still shown as unavailable even if this SSH version has been configured.
Examples	`DGS-3610# show ip ssh`

Related commands

Command	Description
Ip ssh version {**1	2**}	Configure version information for the SSH Server.
ip ssh time-out time	Set the timeout value of user authentication by SSH Server.
Ip ssh authentication-retries retry times	Set the authentication retry times of SSH Server user authentication.

Version description	The software version must be later than v10.1.

43.2.2 show ssh

Show information about each established SSH connection.

show ssh

Parameter description	None
Default configuration	None
Command mode	Privilege mode.
Usage guidelines	Show information about established SSH connections, including VTY number of occupied for connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.
Examples	`DGS-3610# show ssh`
Related commands	None
Version description	The software version must be later than v10.1.

43.2.3 show crypto key mypubkey

Sow information about the public key part of the SSH Server public key.

show crypto key mypubkey *{rsaldsa}*

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	None
Command mode	Privilege mode
Usage guidelines	Sow information about the public key part of the generated SSH Server public key, including key generation time, key name, contents in the public key part, etc.
Examples	`DGS-3610# show crypto key mypubkey rsa`

Related commands

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

Version description	The software version must be later than v10.1.

43.2.4 disconnect ssh

Disconnect the established SSH connection session.

disconnect ssh [vty] *session-id*

Parameter description

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

Default configuration	None
Command mode	Privilege mode.
Usage guidelines	Disconnect the established SSH connection by entering the specified SSH connection session ID. Alternatively, disconnect the specified SSH connection by entering the specified VTY connection session ID. Only connections of the SSH type can be disconnected.

Examples

```
DGS-3610# disconnect ssh 1
```
Or
```
DGS-3610# disconnect ssh vty 1
```

Related commands

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

Version description

The software version must be later than v10.1.

44 Configuring CPU Protection Command

44.1 Configuration Related Commands

There are the following configuration commands for system attack protection:

- **cpu-protect type** *packet-tpye* **pps** *pps_value*
- **cpu-protect type** *packet-tpye* **pri** *pri_value*

44.1.1 cpu-protect type packet-type pps pps_value

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 of the CPU for each type of packet is 1000.

Command mode

Global configuration mode.

Examples

The following example sets the bandwidth for the CPU for receiving BPDU packets:

```
DGS-3610(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 specified type of packets the CPU port receives

Caution

The non-inteligent card of S66 series devices, such as 1X and 6sfp on-line card end don't support the cpp function.

44.1.2 cpu-protect type packet-type pri *pri*_num

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	ID, the value range is 0-7

Default The default is 0 for the queue of each type of packet.

Command mode Global configuration mode.

Examples The following example sets the PBDU packets to queue 7:

```
DGS-3610(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 specified type of packets

44.2 Showing Related Command

The following commands are used to show CPU protection:

- **show cpu-protect mboard**
- **show cpu-protect slot** *slot-id*
- **show cpu-protect type** *packet-type*

44.2.1 show cpu-protect mboard

Show the statistics of the various packets of CPU protection of the management board.

show cpu-protect mboard

Command mode	Privilege mode.
Usage guidelines	This command shows the statistics of the packets currently received by the CPU of the management board.
Examples	The following example shows the CPU protection statistics of the s9610 management board.

```
DGS-3610# 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
 unknow-ipmc     0         0        0
 ttl1            0         0        0
...
```

Related commands

Command	Description
show cpu-protect slot *slot-num*	Show the CPU protection statistics of the specified line card

44.2.2 show cpu-protect slot

Show the CPP statistics of the specified line card.

show cpu-protect slot *slot_num*

Parameter description

Parameter	Description
slot_num	The value range is 1-16.

Command mode	Privilege mode.
Usage	Show the CPP statistics of the specified line card.

guidelines

Examples

The following example shows the CPU protection information of the line card in slot 2.

```
DGS-3610(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
 unknow-ipmc   200        0        0
 ttl1          20         3        0
```

Related commands

Command	Description
show cpu-protect mboard	Show the CPU protect information of the management board

Caution

The non-inteligent card of S66 series devices, such as 1X and 6sfp on-line card end don’t support the cpp function. The online card end doesn't show the statistic information.

When the S66 series device enable the function of igmp snooping, the statistic valule of unknow-ipmc on the line card end.

There is no igmp statistic value on the online card when the multicast function is enabled.

44.2.3 show cpu-protect type

Set 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

Privilege 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:

```
DGS-3610(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 type *packet-type*	Show the statistics of the packets of a specified type of CPU protection.

45 Configuring Anti-attack System Guard command

45.1 Configuration Related Commands

There are the following configuration commands for system anti-attack protection:

- **system-guard enable**
- **system-guard isolate-time seconds**
- **system-guard same-dest-ip-attack-packets number**
- **system-guard same-dest-ip-attack-packets number**
- **system-guard detect-maxnum number**
- **system-guard exception-ip ip mask**
- **clear system-guard [interface interface-id [ip-address ip-address]]**

45.1.1 system-guard enable

Enable the anti-attack function. The **no** format of the command disables the anti-attack function.

Parameter description	This command has no parameters.
Default	The anti-attack function is disabled.
Command mode	Interface configuration mode.
Usage guidelines	

Examples

Enable the anti-attack function

```
DGS-3610(config-if)# system-guard enable
```

Disable the anti-attack function

```
DGS-3610(config-if)# no system-guard enable
```

Related commands

Command	Description
show system-guard	Show the current anti-attack function configuration.

45.1.2 system-guard isolate-time seconds

Configure the isolated time of unauthorized attack user. Use the **no** form of the command to restore the default value.

Parameter description

Parameter	Description
seconds	Isolated time for unauthorized attack users. This IP will restore the communication automatically after it is isolated for a period of time. Its value range is 30s – 3600s, 120s by default.

Default

The default isolated time is 120 seconds.

Command mode

Interface configuration mode.

Usage guidelines

The isolated time for unauthorized attack user is configured. No communication is allowed for the isolated IP within the period of *second*. This IP will restore the communication automatically after this period of time.

Examples

Configure the isolated time as 100 seconds in the interface configuration mode

```
DGS-3610(config-if)# system-guard isolate-time 100
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.1.3 system-guard same-dest-ip-attack-packets number

Configure the maximum threshold of the attack for scanning inexistent IP. Use the **no** form of the command to restore the default value.

Parameter description

Parameter	Description
number	The maximum threshold of the attack that some IP which doesn't exist sends the IP message continuously. The value range is 1 – 2000 messages per second, 20 by default. Setting to 0 indicates this attack is not monitored.

Default

The default value is 20.

Command mode

Interface configuration mode.

Usage guidelines

The less the threshold is set, the poorer the accuracy of the judging for the attacked host is. It is easy to isolate the normal host online incorrectly. It is recommended that administrators to configure corresponding threshold according to the security degree of the actual network environment.

Examples

Configure the maximum threshold as 100 in the interface configuration mode

```
DGS-3610(config-if)# system-guard
same-dest-ip-attack-packets 100
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.1.4 system-guard scan-dest-ip-attack-packets number

Configure the maximum threshold of the attack for scanning a batch of IP network segment. Use the **no** form of the command to restore the default value.

Parameter description

Parameter	Description
number	Configure the maximum threshold of the attack for scanning a batch of IP network segment. The value range is 1 – 2000 messages per second, 10 by default. Setting to 0 indicates this attack is not monitored.

Default

The default value is 10.

Command mode

Interface configuration mode.

Usage guidelines

The less the threshold is set, the poorer the accuracy of the judging for the attacked host is. It is easy to isolate the normal host online incorrectly. It is recommended that administrators to configure corresponding threshold according to the security degree of the actual network environment.

Examples

Configure the maximum threshold as 100 in the interface configuration mode

```
DGS-3610(config-if)# system-guard
scan-dest-ip-attack-packets 100
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.1.5 system-guard detect-maxnum number

Set the maximum quantity of attacked hosts. Use the **no** form of the command to restore the default value.

Parameter description

Parameter	Description
num	Configure the maximum threshold of the attack for scanning a batch of IP network segment. The value range is 1 – 2000 messages per second, 10 by default. Setting to 0 indicates this attack is not monitored.

Default	The default value is 100.
Command mode	Global configuration mode.
Usage guidelines	In general, this quantity should be maintained as the quantity of the actual operated hosts divided by 20. However, if you detect that the isolated hosts reach or approach to the maximum quantity of the monitored hosts, the quantity of the monitored hosts can be enlarged to meet the requirement for better system guard. Note: If you change the quantity of the monitored hosts to be less than original quantity, it will cause the data of current monitored host to be cleared.
Examples	Set the maximum quantity of the attacked hosts as 200 in the global configuration mode. `DGS-3610(config)# system-guard detect-maxnum 200`

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.1.6 system-guard exception-ip ip mask

Set exceptional IPs free from monitoring. Use the **no** form of the command to restore the default value.

Parameter description

Parameter	Description
ip	Dotted decimal ip address
mask	Dotted decimal mask
all-eip	Delete all exceptional IPs. This option is used for the **no** command only.

Default	No exceptional IP
Command mode	Global configuration mode.
Usage guidelines	This command is used to add an exceptional IP for the anti-attack function to allow its access to the interface.

Examples

In the global configuration mode, set the exceptional IP: 192.168.5.145 255.255.255.0 that is not monitored.

```
DGS-3610(config-if)# system-guard exception
192.168.5.145 255.255.255.0
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.1.7 clear system-guard [interface interface-id [ip-address ip-address]]

Clear the isolated IPs

Parameter description

Parameter	Description
interface *interface-id*	Interface
ip-address *ip-address*	IP address

Default

None

Command mode

Privileged mode.

Usage guidelines

Examples

Clear the isolated IPs in the port **fastethernet** 0/1:

```
DGS-3610(config)# clear system-guard interface
fastethernet 0/1
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.2 Showing Related Command

There are the following configuration commands for system attack protection:

- **show system-guard [interface *interface-id*]**
- **show system-guard isolate-ip [interface *interface-id*]**
- **show system-guard detect-ip [interface *interface-id*]**
- **show system-guard exception-ip**

45.2.1 show system-guard [interface *interface-id*]

Check the configuration parameters of anti-attack system guard.

Parameter description

Parameter	Description
interface *interface-id*	Interface

Default

None

Command mode

Privileged mode.

Usage guidelines

Examples

```
DGS-3610# show system-guard
detect-maxnum number   : 100       //Maximum number of hosts
monitored by the device
isolated host number   : 11        //Number of hosts isolated by
the device
inteface  state  isolate time  same-attack-pkts  scan-attack-pkts
--------------------- ---------------   ------------------
Fa 0/1    ENABLE    120             20                 10
Fa 0/2    DISABLE   110             21                 11
……
DGS-3610# show system-guard interface Fa 0/1
detect-maxnum number   : 100       //Maximum number of hosts
monitored by the device
isolated host number   : 11        //Number of hosts isolated by
the device
inteface  state  isolate time  same-attack-pkts  scan-attack-pkts
---------------------- ---------------   ------------------
Fa 0/1    ENABLE    120             20                 10
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.2.2 show system-guard isolate-ip [interface *interface-id*]

Check the information of isolated IPs of the interface for anti-attack system guard

Parameter description

Parameter	Description
interface *interface-id*	Interface

Default None

Command mode Privileged mode.

Usage guidelines

Examples

```
DGS-3610# show system-guard isolated-ip
interface   ip-address    isolate reason   remain-time(second)
---------  -------------  ---------------  ------------------
Fa 0/1    192.168.5.119   scan ip attack     110
Fa 0/1    192.168.5.109   same ip attack     61
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.2.3 show system-guard detect-ip [interface *interface-id*]

View the IP that is being monitored.

Parameter description

Parameter	Description
interface *interface-id*	Interface

Default None

Command mode

Privileged mode.

Usage guidelines

Examples

```
DGS-3610# show system-guard detect-ip
interface  ip-address  same ip attack packets  scan ip attack
packets
-----------------------------------------------------
Fa 0/1    192.168.5.118         0              8
Fa 0/1    192.168.5.108        12              2
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function of the interface

45.2.4 show system-guard isolate-ip [interface *interface-id*]

To show the exceptional IPs that allow device access in the anti-attack function.

Parameter description

Parameter	Description
interface *interface-id*	Interface

Default

Command mode

Privileged mode.

Usage guidelines

Examples

```
DGS-3610# show system-guard exception-ip
Exception IP Address    Exception Mask
--------------------  ---------------
255.255.255.0
192.168.4.11           255.255.255.0
```

	Command	Description
Related commands	**system-guard enable**	Enable the anti-attack function of the interface

46 Configuring GSN Security Solution Command

46.1 Configuration related command

Global configuration mode command.

- **security gsn enable**
- **security community**
- **snmp-server host**
- **scurity event interval**

Interface mode commands:

- **security address-bind enable**

46.1.1 security gsn enable

This command allows you to enable the global GSN. Its **no** form allows you to disable this function.

security gsn enable

no security gsn enable

Parameter description		None

Default configuration		Off

Command mode	Global configuration mode.
Usage	When the device needs to support the GSN security solution, you can

guidelines	enable the equipment to support the GSN security solution by configuring this command
Examples	DGS-3610# **configure terminal** DGS-3610(config)# **security gsn enable**
Related commands	None
Platform description	The software version must be later than v10.1.

46.1.2 security community

This command allows you to configure the security name for communication with the smp server.

security { [**v1** | **v2**] **community** *community* | **v3 user** *username* }

no security { [**v1** | **v2**] **community** *community* | **v3 user** *username* }

Parameter description

Parameter	Description
community	*community* string for interacting with the server.
username	v3 security communication name used.

Default configuration		No configuration.
Command mode		Global configuration mode.
Usage guideline		When you need to configure the communication between the equipment and server, you need to select the appropriate protocol version according to the configuration of the server and configure the appropriate authentication name. If v3 is selected, you need to configure the related v3 user name by using the snmp-server command. For details, see the SNMP command reference.

Examples		Configure v1 community:
		`DGS-3610(config)# security v1 community public`
		Configure **start** as the v3 user name:
		`DGS-3610(config)# security v3 user start`

Related commands		None

Platform description		The software version must be above v10.1.

46.1.3 smp-server host

This command allows you to configure the **ip** address of the corresponding smp-server.

smp-server host *ip-address*

no smp-server host

Parameter description		**Parameter**	**Description**
		ip-address	**ip** address of the SMP Server

Default configuration		No smp server is configured.

Command mode		Global configuration mode.

Usage guideline		Execute this command. You can view the settings by using the **show smp-server** command.

Examples		`DGS-3610(config)#smp-server host 192.168.4.243`

Related commands		**Command**	**Description**
		show smp-server	Show the configuration of the SMP server

Platform description		The software version must be later than v10.1.

46.1.4 security event inteval

This command allows you to configure the minimum transmission interval of the equipment.

security event inteval *interval*

no security event inteval

Parameter description		**Parameter**	**Description**
		interval	Interval of the security event

Default configuration		5

Command mode		Global configuration mode.

Usage guideline		Execute this command. You can view the settings by using the **show security event interval** command.

Examples		Configure the minimum interval of the security event: `DGS-3610(config)# **security event interval** *10*`

Related commands		**Command**	**Description**
		show security event interval	Show the minimum interval of the security event

Platform description		The software version must be later than v10.1.

46.1.5 security address-bind enable

This command allows you to configure whether to enable the address binding policy on the port of the equipment.

security address-bind enable

no security address-bind enable

Parameter description		None

Default configuration		None

Command mode		Interface mode, supporting the common L2 switching port (excluding AP and AP member port)

Usage guideline		Execute this command .The address binding of the port is enabled. Please note that this command can only be used when the global GSN is enabled.

Examples		Configure the minimum interval of the security event: `DGS-3610(config-if)# security address-bind enable`

Related commands		**Command**	**Description**
		security gsn enable	Enable global GSN

Platform description		The software version must be later than v10.1.

46.2 Showing and Monitoring Commands

Showing and monitoring include the following commands:

show smp-server

show security event interval

46.2.1 show smp-server

Show the IP address of the SMP Server.

Parameter description		None

Command mode		Privilege mode.

Usage guideline		Show the IP address of the SMP Server.

Examples		DGS-3610# **show smp-server** SMP-Server IP: 192.168.20.30

Related commands		**Command**	**Description**
		smp-server host	Configure the smp server ip address

Platform description		The software version must be later than v10.1.

46.2.2 show security evnet interval

Show the minimum interval of the security event.

Parameter description		None

Command mode		Privilege mode.

Usage guideline		Show the minimum interval of the security event.

Examples	DGS-3610# **show security event interval** Event sending interval(Seconds):5

Related commands	**Command**	**Description**
	security event interval *interval*	Configure the minimum interval of the security event

Platform description	The software version must be later than v10.1.

47 Configuring DAI Commands

47.1 Enable and Disable DAI Function Commands

The configuration commands are as follows:

- **ip arp inspection**

47.1.1 ip arp inspection

This command is used to configure whether the DAI function is enabled, and the no option of this command can be used to disable the DAI function. The command format is as follows:

ip arp inspection

no ip arp inspection

Parameter description	No parameters
Default	The DAI function is not enabled.
Command mode	Global configuration mode.
Usage guidelines	The enable/disable of the DAI will not depend on other configuration commands of the DAI function. When the DAI function is disabled, the ARP message that needs to forward within the VLAN is carried out by the hardware. When the DAI function is enabled, the hardware will not forward the ARP message and all messages to be forwarded or sent to the equipment will be delivered to the DAI module toe carry out the validity check.The message will be processed further if it is qualified, otherwise, this message will be discarded. The enabling of the DAI function will reduce the performance of the equipment.

Examples

```
DGS-3610(config)# ip arp inspection
```

Related commands

Command	Description
show running-config	Show whether the DAI function is enabled.

47.2 Enable and Disable DAI Packet Inspection Function of Specified VLAN Commands

This configuration command includes:

- **ip arp inspection vlan**

47.2.1 ip arp inspection vlan *vlan-id*

Use this command to enable the DAI function of VLAN corresponding to the vlan-id. The no option of this command can disable the DAI function of VLAN corresponding to the vlan-id. If the parameter vlan-id is neglected, the DAI 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	Indicates the vlan ID.

Default

The DAI function of all VLANs is disabled.

Command mode

Global configuration mode.

Usage guidelines

To make this command play its role, enable the DAI function firstly. Refer to above section.

Examples

The following configuration is to check the ARP packet received from the VLAN 1.

```
DGS-3610(config)# ip arp inspection
DGS-3610(config)# ip arp inspection vlan 1
```

Related

Command	Description

commands	**show ip arp inspection vlan**	Show whether VLAN enables the DAI function.

47.3 Whether L2 Port Is/Is not Trustable Configuration Commands

47.3.1 ip arp inspection trust

To configure whether the L2 port is trustable, use the interface configuration command **ip arp inspection trust**. The no option of this command will restore the L2 port to the trustless status.

ip arp inspection trust

no ip arp inspection trust

Parameter description	
Default configuration	The port is in the trustless status.
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, can set it in the trusted status, to indicate that we need not check whether the ARP message received by this interface is legal.

Examples	The configuration example below sets the gigabitEthernet 0/19 port as the trust.
	`DGS-3610(config)# interface gigabitEthernet 0/19`
	`DGS-3610(config-if)# ip arp inspection trust`

Related commands	**Command**	**Description**
	show ip arp inspection interface	Show the IP routing table

47.4 Configuration of the Limit Receiving Rate of ARP Message at L2 Port

The configuration related commands include as follows:

- **ip arp inspection limit-rate**

47.4.1 ip arp inspection limit-rate *limit-rate*

To define the limit rate of ARP message received by one interface, use the interface configuration command **ip arp inspection limit-rate:** The no option of this command is used to restore the default configuration.

ip arp inspection limit-rate {*limit-rate* | **none** }

no ip arp inspection limit-rate

Parameter description

Parameter	Description
none	This interface is not limited by the rate.
limit-rate	The limit rate, whose range is (1, 2048).

Default

The default limit rate of the trustless port is 15 ARP messages per second.

Command mode

Interface configuration mode

Usage guidelines

Only when the DAI function is enabled, the limit rate will take into effect;

Examples

In the configuration example below, the configuration rate for the interface gigabitEthernet 0/2 of VLAN 2 is limited to 10 ARP message per second.

```
DGS-3610(config)# ip arp inspection
DGS-3610(config)# interface gigabitEthernet 0/2
DGS-3610(config-if)# ip arp inspection limit-rate 10
```

47.5 DHCP Snooping Database Related Configuration

If the DAI function is enabled, the corresponding DAI funciton of the VLAN is enabled and the L2 port which receives the ARP message is in the trustless status, carrry out the validity check for the ARP message, the check foudation is that the DHCP Snooping database related information will pass the check if no configuration is carried out for the database.For the configuration on the DHCP Snooping, refer to the *DHCP Snooping Configuration*.

48 Configuring ACL Commands

For IDs used in the following commands, refer to the command ID table below:

ID	Meaning
id	Number of access list. Range: IP standard ACL: 1-99,1300-1999 IP extended ACL: 100-199,2000-2699 MAC extended ACL: 700–799 Extended expert ACL: 2700–2899
name	ACL name
sn	ACL SN (products can be set according to the priority)
start-sn	Start sequence
inc-sn	Sequence increment
deny	If matched, access is denied.
permit	If matched, access is permitted.
prot	Protocol number. For IPv6, this field can be ipv6, icmp, tcp, udp and numbers 0-255. For IPv4, it can be one of eigrp, gre, ipinip, igmp, nos, ospf, icmp, udp, tcp, and ip, or it can be numbers 0-255 that represent the IP protocol. It is described when some important protocols, such as icmp/tcp/udp, are listed individually.
interface *idx*	Enter the matched interface
src	Packet source address (host address or network address)
src-wildcard	Source 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 *dscp*	Differential service code point, and code point value. Range: 0-63
flow-label flow-label	Flow label. Value range: 0-1048575
dst	Packet destination address (host address or network address)

ID	Meaning
dst-wildcard	Destination address wildcard.It can be discontinuous, such as 0.255.0.32
fragment	Packet fragment filtering
precedence *precedence*	Packet precedence value (0-7)
time-range *tm-rng-name*	Time range of packet filtering, named *tm-rng-name*
tos *tos*	Service type of packet (0-15)
cos *cos*	cos value of packet (0-7)
cos inner *cos*	cos of the tag inner the message
icmp-type	ICMP packet message type (0-255)
icmp-code	ICMP packet message type code (0-255)
icmp-message	ICMP packet message type name (0-255)
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 source host
dst-mac-addr	Physical address of destination host
VID vid	Specified vlan id
VID inner vid	Specity the vid inner tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all *tcpf*	Match all bits of tcp flag
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{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
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.

48.1 Configuration Related Commands

Global configuration mode commands:

- **access-list**
- **ip access-list**
- **mac access-list**
- **expert access-list**
- **ipv6 access-list**
- **ip access-list resequence**

ACL configuration mode commands:

- **deny**
- **permit**

- **list-remark text**
- **no sn**

Interface mode commands:

- **ip access-group**
- **mac access-group**
- **expert access-group**
- **ipv6 traffic-filter**

48.1.1 access-list

This command creates an access list rule to filter data packets. The **no** form of this command deletes the specified access list entries.

Caution The NPE80 supports only the standard and extended IP access list, and can match only the quintuple. The information other than quintuple such as TOS is not supported.

1. Standard IP access list (1-99, 1300-1999)

   access-list *id* {**deny** | **permit**} {**source** *source-wildcard* | **host** *source* | **any**}

2. Extended IP access list (100-199, 2000-2699)

   access-list *id* {**deny** | **permit**} **protocol** {**source** *source-wildcard* | **host** *source* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*]

3. Extended MAC access list (700-799)

   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 (2700-2899)

   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*] [**fragments**] [**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*]

[fragments] [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*] [**fragments**]

[**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*] [**fragments**] [**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*] [**fragments**] [**time-range** *time-range-name*]

5. List notes

access-list list-remark text

The following parameter description describes the parameters in the sequence they appear. The parameters once described will not be further described when they appear in the configuration statements later.

Parameter description

Parameter	Description
id	Access list ID. The ranges available are 1-99, 100-199, 1300-1999, 2000-2699, 2700-2899, and 700-799.
deny	If not matched, access is denied.

Permit	If matched, access is permitted.
Source	Packet source 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	Packet destination address (host address or network address)
destination-wildcard	Wildcard of the destination address. It can be discontinuous, for example, 0.255.0.32.
fragments	Packet fragment filtering
precedence	Packet priority level
precedence	Packet precedence value (0-7)
time-range	Time range of packet filtering
time-range-name	Time range name of packet filtering
tos	Type of service of the packet
tos	ToS value (0-15)
icmp-type	ICMP packet message type (0-255)
icmp-code	ICMP packet message type code (0-255)
icmp-message	ICMP packet 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*	One of the source host Physical address
host *destination-mac-address*	Physical address of the destination address
VID *vid*	Match specified VID
ethernet-type	Ethernet protocols type
match-all	Match all the bits of the tcp flag
tcp-flag	tcp flag

Default configuration

No any ACL.

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 (1-99, 1300-1999) only controls the source addresses.

The extended IP ACL (100-199, 2000-2699) can enforce strict control over the source and destination addresses.

The extended MAC ACL (700-799) can match according to the source/destination mac addresses and Ethernet type. The extended expert access list (2700-2899) is a combination of the above and can match and filter the VLAN id.

The Tcp Flag includes part or all of the following:

- **urg**
- **ack**
- **psh**
- **rst**
- **syn**
- **fin**

The packet precedence names are as below:

- **critical**

- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The service type names are as below:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The ICMP packet message type names 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**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **ttl-exceeded**
- **unreachable**

Below are the TCP port names. The TCP can specify ports according to the port names and port numbers:

- **bgp**
- **chargen**
- **cmd**
- **daytime**
- **discard**
- **domain**
- **echo**
- **exec**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **ident**
- **irc**
- **klogin**
- **kshell**
- **login**
- **nntp**
- **pim-auto-rp**
- **pop2**
- **pop3**

- **smtp**
- **sunrpc**
- **syslog**
- **tacacs**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

Below are the UDP port names. The UDP can specify ports according to the port names and port numbers:

- **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-type is shown 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 addresses are 192.168.1.64 - 192.168.1.127 to pass and other packets are denied:

```
DGS-3610(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 packets and ICMP packets to pass:

```
DGS-3610(config)# access-list 102 permit tcp any any eq domain
DGS-3610(config)# access-list 102 permit udp any any eq domain
DGS-3610(config)# access-list 102 permit icmp any any echo
DGS-3610(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 MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 0/1. The configuration procedure is as below:

```
DGS-3610(config)#access-list 702 deny host 00d0f8000c0c any aarp
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(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.

```
DGS-3610(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
DGS-3610(config)# access-list 2702 permit any any any any
DGS-3610(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

Platform description

The software version must be later than v10.0.

48.1.2 ip access-list

Use this command to create standard IP ACL or extended IP ACL, and enter the configuration mode. 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 IP ACL, standard (1-99, 1300-1999), extended (100-199, 2000-2699)
name	Name of IP ACL

Default configuration

No any ACL.

Command mode

Global configuration mode.

Usage guidelines

There are differences between standard ACL and extended ACL, and extended ACLs are more precise. Refer to **deny** or **permit** in the two modes. Use **show ip access-lists** to display the ACL configurations**.**

Examples

Create an extended ACL:

```
DGS-3610(config)# ip access-list extended 123
DGS-3610(config-ext-nacl)# show ip access-lists
ip access-list extended 123
DGS-3610(config-ext-nacl)#
```

Create an extended ACL:

```
DGS-3610(config)# ip access-list standard std-acl
DGS-3610(config-std-nacl)# show ip access-lists
ip access-list standard std-acl
DGS-3610(config-std-nacl)#
```

Related commands

Command	Description
show ip access-lists	Show the IP ACLs.

Platform description

The software version must be later than v10.0.

48.1.3 MAC access-list

Use this command to create extended ACL of MAC , and enter the configuration mode. Use the **no** form of the command to remove the ACL.

mac access-list extended { *id*|name }

no mac access-list extended {*id*|*name*}

Caution

The NPE80 does not support this command.

Parameter description

Parameter	Description
Id	ID of the mac ACL (700-799)
Name	Name of the mac ACL

Default configuration

No any ACL of MAC .

Command mode

Global configuration mode.

Usage guidelines

Execute this command. Use **show ip access-lists** to display the ACL configurations**.**

Examples

Create an extended ACL**:**

```
DGS-3610(config)# mac access-list extended mac-acl
DGS-3610(config-mac-nacl)# show mac access-lists
mac access-list extended mac-acl
DGS-3610(config-mac-nacl)#
```

Create an extended ACL

```
DGS-3610(config)# mac access-list extended 704
DGS-3610(config-mac-nacl)# show mac access-lists
mac access-list extended 704
DGS-3610(config-mac-nacl)#
```

Related commands

Command	Description
show mac access-lists	Show the extended mac ACLs

Platform description

The software version must be later than v10.0.

48.1.4 expert access-list

Use this command to create extended expert ACL, and enter the configuration mode. Use the **no** form of the command to remove the ACL.

expert access-list extended {*id* | *name*}

no expert access-list extended {*id* | *name*}

Caution

The NPE80 does not support this command.

Parameter description

Parameter	Description
Id	Item of the Expert ACL (2700-2899)
Name	Name of the ACL

Default configuration

No Expert ACL

Command mode	Global configuration mode.
Usage guidelines	Execute this command. Use the **show expert access-lists** command to display the ACL configurations**.**

Examples	Create an extended expert ACL:
	`DGS-3610(config)# expert access-list extended exp-acl`
	`DGS-3610(config-exp-nacl)# show expert access-lists`
	`expert access-list extended exp-acl`
	`DGS-3610(config-exp-nacl)#`
	
	Create an extended expert ACL:
	`DGS-3610(config)# expert access-list extended 2704`
	`DGS-3610(config-exp-nacl)# show expert access-lists`
	`expert access-list extended 2704`
	`DGS-3610(config-exp-nacl)#`

Related commands

Command	Description
show expert access-lists	Show the extended expert ACLs

Platform description	The software version must be later than v10.0.

48.1.5 ipv6 access-list

Use this command to create extended IPV6 ACL, and enter the configuration mode. Use the **no** form of the command to remove the ACL.

ipv6 access-list extended *name*

no ipv6 access-list extended *name*

Caution

NPE80 does not support this command.

Parameter description

Parameter	Description
name	ACL name

Command mode	Global configuration mode.
Usage guidelines	Execute this command. Use **show ipv6 access-lists** to display the ACL configurations**.**

Examples	Create an extended ipv6 ACL**:**
	`DGS-3610(config)# expert access-list extended v6-acl`
	`DGS-3610(config-ipv6-nacl)# show ipv6 access-lists`
	`ipv6 access-list extended v6-acl`
	`DGS-3610(config-ipv6-nacl)#`

Related commands

Command	Description
show ipv6 access-lists	Show the extended ipv6 ACLs

Platform description	The software version must be later than v10.0.

48.1.6 ip access-list resequence

This command resequences the ACL entries of IP type, creates extended IPV6 ACLs, and enters this configuration mode. You can use the **no** form of this command to restore 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	*start-sn:* 10 *inc-sn:* 10
Command mode	Global configuration mode.

Usage guidelines	Execute this command. Use the **show access-lists** command to display the ACL configurations**.**

Examples

Resequence the entries of the ACL:

```
DGS-3610# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
DGS-3610# config
DGS-3610# (config)#ip access-list resequence 1 21 43
DGS-3610# (config)#exit
DGS-3610# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
DGS-3610#
```

Related commands

Command	Description
show access-lists	Show the ACLs

Platform description	The software version must be later than v10.0.

48.1.7 deny

Declare one or more deny conditions to decide whether the packets are forwarded or discarded. In the ACL configuration mode, modify the existing ACL or set the particulars of the protocol.

Caution

The NPE80 only supports the standard and extended IP access list, and can only match the quintuple. The information other than quintuple such as TOS is not supported.

1. Standard IP ACL

   [*sn*] **deny** {**source** *source-wildcard* | **host** *source* | **any**}

2. Extended IP ACL

   [*sn*] **deny protocol source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*]

Extended IP ACLs of some important protocols:

- **Internet Control Message Protocol** (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*] [**fragments**] [**time-range** *time-range-name*]

- **Transmission Control Protocol**(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*] [**fragments**] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (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*] [**fragments**] [**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*][**fragments**] [**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*]

  [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**time-range** *time-range-name*]

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] [**fragments**] [**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] [**fragments**] [**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*] [**fragments**] [**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*]
[**fragments**] [**time-range** *time-range-name*]

Parameter description

Parameter	Description
For the parameters not metioned below, please refer to the **access-list**	
Sn	ACL entry 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	DSCP code, within the range of 0-63.
flow-label	Flow label
flow-label	Flow label value, within the range of 0-1048575.
protocol	For the ipv6, the field can be ipv6 | icmp | tcp | udp and <0-255>

Default configuration

No any entry

Command mode

ACL configuration mode.

Usage guidelines

Configure the filtering condition entry of the ACL in the ACL configuration mode

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.

```
DGS-3610(config)# expert access-list extended 2702
DGS-3610(config-exp-nacl)#deny tcp  host
192.168.4.12 host 0013.0049.8272 any any
DGS-3610(config-exp-nacl)#permit any any any any
DGS-3610(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
DGS-3610(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the source host with the IP address 192.168.4.12 to provide service with the TCP port 100 and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)# ip access-list extended ip-ext-acl
DGS-3610(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
DGS-3610(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
DGS-3610(config-ext-nacl)#exit
DGS-3610(config)#interface gigabitethernet 1/1
DGS-3610(config-if)#ip access-group ip-ext-acl in
DGS-3610(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the source host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)#mac access-list extended mac1
DGS-3610(config-mac-nacl)#deny host 0013.0049.8272 any aarp
DGS-3610(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
DGS-3610(config-mac-nacl)#exit
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the source host with the IP address 192.168.4.12 and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)# ip access-list standard 34
DGS-3610(config-ext-nacl)# deny host 192.168.4.12
DGS-3610(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
```

```
DGS-3610(config-ext-nacl)#exit
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# ip access-group 34 in
```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the source host with the IP address 192.168.4.12 and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)#ipv6 access-list extended v6-acl
DGS-3610(config-ipv6-nacl)#11 deny ipv6 host 192.168.4.12 any
DGS-3610(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
DGS-3610(config-ipv6-nacl)# exit
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# ipv6 traffic-filter v6-acl in
```

Related commands

Command	Description
show access-list	View 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 entry definitions

Platform description

The software version must be later than v10.0.

48.1.8 permit

Declare one or more permitted (**permit)** conditions to decide whether the packets are forwarded or discarded. In the ACL configuration mode, modify the existing ACL or set the particulars of the protocol.

Caution The NPE80 only supports the standard and extended IP access list, and can only match the quintuple. The information other than quintuple such as TOS is not supported.

1. Standard IP ACL

   [*sn*] **permit** {**source** *source-wildcard* | **host** *source* | **any**}

2. Extended IP ACL

   [*sn*] **permit protocol source** *source-wildcard* **destination**

   destination-wildcard [**precedence** *precedence*] [**tos** *tos*] **[fragments**]

   [**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*] [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**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*][**fragments**] [**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*]

  [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**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] [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**time-range** *time-range-name*]

Parameter description	For those not listed below, see deny.
Default configuration	No any entry.
Command mode	ACL configuration mode.
Usage guidelines	Configure the permit condition entry of the ACL in the ACL configuration mode

Examples	The following example shows how to create and display an Extended expert ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.
	`DGS-3610(config)#expert access-list extended exp-acl`
	`DGS-3610(config-exp-nacl)#permit tcp host 192.168.4.12 host 0013.0049.8272 any any`
	`DGS-3610(config-exp-nacl)#deny any any any any`
	`DGS-3610(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
DGS-3610(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the source host with the IP address 192.168.4.12 to provide service with the TCP port 100 and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)# ip access-list extended 102
DGS-3610(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
DGS-3610(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
DGS-3610(config-ext-nacl)# exit
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)#ip access-group 102 in
DGS-3610(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the source host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)# mac access-list extended 702
DGS-3610(config-mac-nacl)# permit host 0013.0049.8272 any aarp
DGS-3610(config-mac-nacl)# show access-lists
mac access-list extended
10 permit host 0013.0049.8272 any aarp 702
DGS-3610(config-mac-nacl)# exit
DGS-3610(config)#interface gigabitethernet 1/1
DGS-3610(config-if) #mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the source host with the IP address 192.168.4.12 and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)# ip access-list standard std-acl
DGS-3610(config-std-nacl)# permit host 192.168.4.12
DGS-3610(config-std-nacl)# show access-lists
ip access-list standard std-acl
10 permit host 192.168.4.12
DGS-3610(config-std-nacl)# exit
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL. The purpose is to permit the source host with the IP address 192.168.4.12

and apply to Interface 1. The configuration procedure is as below:

```
DGS-3610(config)# ipv6 access-list extended v6-acl
DGS-3610(config-ipv6-nacl)# 11 permit ipv6
host ::192.168.4.12 any
DGS-3610(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
DGS-3610(config-ipv6-nacl)# exit
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(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	Define the deny ACL entry

Platform description

The software version must be later than v10.0.

48.1.9 list-remark text

Add remarks for the specified ACL. The **no** form deletes the prefix.

list-remark *text*

Parameter description

Parameter	Description
Text	Remark text

Command mode

ACL configuration mode.

Usage

Add remarks for the specified ACL.

guidelines

Examples

```
DGS-3610# ip access-list extended 102
DGS-3610(config-ext-nacl)# list-remark this acl is to filter the
host 192.168.4.12
DGS-3610(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
DGS-3610(config-ext-nacl)#
```

Related commands

Command	Description
show access-list	Show the ACLs
ip access-list	Define the IP ACL

Platform description

The software version must be later than v10.0.

48.1.10 no sn

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

Delete the ACL entry in the ACL configuration mode.

Examples

```
DGS-3610(config)# ipv6 access-list extended v6-acl
DGS-3610(config-ipv6-nacl)# permit ipv6 host ::192.168.4.12 any
DGS-3610(config-ipv6-nacl)# 12 deny ipv6 host any any
DGS-3610(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
```

```
DGS-3610(config-ipv6-nacl)# no 12
DGS-3610(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
DGS-3610(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 ACL entry
permit	Define the permit ACL entry

Platform description The software version must be later than v10.0.

48.1.11 ip access-group

To apply a specific ACL to an interface, please execute the **ip access-group** interface configuration command. The **no** form of this command cancels the association between the ACL and the interface.

ip access-group {*id* | *name*} {**in | out**}

no ip access-group {*I d*| *name*} {**in | out**}

Caution The NPE80 only supports the filtering of the packets inputting to the interface, it does not support the filtering of the packets outputting to the interface.

Parameter description

Parameter	Description
id	ID of the IP ACL (1-199, 1300-2699)
name	Name of IP ACL
in	Filter the ininputting packets of the interface
out	Filter the outputting packets of the interface

Default configuration The interface is not applied with any ACL.

Command mode	Interface configuration mode
Usage guidelines	Use the **ip access-group** command to apply the ACL to an interface, and the firewall is enabled.

Examples	The following example applies the ACL 120 on the fastEthernet0/0 to filter the inputting packets:
	`DGS-3610(config)# interface fastEthernet 0/0`
	`DGS-3610(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 (1-199, 1300 – 2699, 3000-3199)

Platform description	The software version must be later than v10.0.

48.1.12 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 configurations.

mac access-group {*id* | *name*}{**in | out**}

no mac access-group {*id* | *name*} {**in | out**}

Caution The NPE80 does not support this command.

Parameter description

Parameter	Description
id	ID of the IP ACL (700-799)
name	Name of IP ACL
in	Filter the inputting packets of the interface

	out	Filter the outputting packets of the interface

Default configuration

The interface is not applied with any ACL.

Command mode

Interface configuration mode.

Usage guidelines

Apply the ACL to the packets of the interface. Use **show running-config** to display configuration.

Examples

The following example shows how to apply the access-list accept_00d0f8xxxxxx only to Gigabit interface 1:

```
DGS-3610(config)# interface GigaEthernet 1/1
DGS-3610(config-if)# mac access-group accept_00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Use this command to bind the ACL configurations.

Platform description

The software version must be later than v10.0.

48.1.13 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 configurations.

expert access-group {*id* | *name*} {**in | out**}

no expert access-group {*id* | *name*} {**in | out**}

Caution

The NPE80 does not support this command.

Related commands

Command	Description
id	ID of the IP ACL (2700-2899)
name	Name of IP ACL

	in	Filter the inputting packets of the interface
	out	Filter the outputting packets of the interface

Default configuration

The interface is not applied with any Expert ACL.

Command mode

Interface configuration mode.

Usage guidelines

Apply the specified ACL interface to the interface for access control over the data streams to the interface. Use **show access-group** to display configuration.

Examples

The following example shows how to apply the access-list *accept*_00d0f8xxxxxx only to Gigabit interface 1:

```
DGS-3610(config)# interface GigaEthernet 0/1
DGS-3610(config-if)# expert access-group accept_00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Use this command to show the bound ACL configurations on the interface.

Platform description

The software version must be later than v10.0.

48.1.14 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 configurations.

ipv6 traffic-filter *name* {**in | out**}

no ipv6 traffic-filter *name* {**in | out**}

Caution

The NPE80 does not support this command.

Related

Command	Description

commands

name	Name of IPV6 ACL.
in	Filter the inputting packets to the interface
out	Filter the outputting packets from the interface

Default configuration

The interface is not applied with any IPv6 ACL.

Command mode

Interface configuration mode.

Usage guidelines

Apply the specified ACL to the interface for controlling the input/output of the data flows to the interface. Use **show access-group** to display configuration.

Examples

The following example shows how to apply the access-list *v6-acl* to Gigabit interface 1:

```
DGS-3610(config)# interface GigaEthernet 0/1
DGS-3610(config-if)# ipv6 traffic-filter v6-acl in
```

Related commands

Command	Description
show access-group	Use this command to show the bound ACL configurations on the interface.

Platform description

The software version must be later than v10.0.

48.2 Showing the Related Commands

Showing and monitoring include the following commands:

- **show access-lists**
- **show ip access-group**
- **show mac access-group**
- **show ipv6 access-group**
- **show expert access-group**
- **Show access-group**

48.2.1 show access-lists

Show all ACLs setting or ACLs of the specified name.

show access-lists [*id*| *name*]

Related commands

Command	Description
id	ID of the ACL.
name	Name of 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

```
DGS-3610# show access-lists n_acl
ip access-list standard n_acl
DGS-3610# show access-lists 102
ip access-list extended 102
DGS-3610# 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 expert ACL
ipv6 access-list	Define the extended IPv6 ACL

Platform description

The software version must be later than v10.0.

48.2.2 show ip access-group

Show the IP ACL configured in the interface.

show ip access-group[**interface** <*interface*>]

Related commands

Command	Description
<interface>	Specified interface.

Command mode

Privileged mode.

Usage guidelines

Show the configured IP ACL of the interface. If not any interface is specified, all the associated IP ACLs of the interfaces will be shown.

Examples

```
DGS-3610# 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

Platform description

The software version must be later than v10.0.

48.2.3 show expert access-group

Show the configured Expert ACL of the interface.

show expert access-group [**interface** <*interface*>]

Caution

The NPE80 does not support this command.

Related commands

Command	Description
<interface>	Specified interface

Command mode

Privileged mode.

Usage guidelines

Show the Expert ACLconfigured of the interface. If not any interface is specified, the associated Expert ACLs of all the interfaces will be shown.

Examples

```
DGS-3610# 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

Platform description

The software version must be later than v10.0.

48.2.4 show mac access-group

Show the configured MAC ACL of the interface.

show mac access-group[**interface** <*interface*>]

Caution

The NPE80 does not support this command.

Related commands

Command	Description
<*interface*>	Specified interface

Command mode

Privileged mode.

Usage guidelines

Show the MAC ACL associated with the interface. If not any interface is specified, the associated MAC ACLs of all associated interfaces will be shown.

Examples

```
DGS-3610# show mac access-group interface gigabitethernet 0/3
mac access-group mm in
Applied On interface GigabitEthernet 0/3.
```

Related commands

Command	Description
mac access-list	Define the extended MAC ACL

Platform description	The software version must be later than v10.0.

48.2.5 show ipv6 access-group

Show the configured IPV6 ACL of the interface.

show ipv6 access-group[**interface** <*interface*>]

Caution

The NPE80 does not support this command.

Parameter description

Parameter	Description
<*interface*>	Specified interface

Command mode	Privileged mode.
Usage guidelines	Show the IPv6 ACL associated with the interface. If not any interface is specified, the associated IPv6 ACLs of all the interfaces will be shown.

Examples

```
DGS-3610# show ipv6 access-group interface gigabitethernet 0/4
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/4.
```

Related commands

Command	Description
ipv6 access-list	Define the extended ipv6 ACL

Platform description	The software version must be later than v10.0.

48.2.6 Show access-group

Use this command to show the ACL configurations bound on the interface.

show access-group [**interface** <*interface*>]

Parameter description

Parameter	Description
<interface>	Specified interface

Command mode

Privileged mode.

Usage guidelines

Show the ACL applied on the interface. If no interface is specified, the ACLs applied on all the interfaces will be shown.

Examples

```
DGS-3610# 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	Define the IP ACL
mac access-group	Define the MAC ACL
expert access-group	Define the Expert ACL
ipv6 traffic-filter	Define the IPv6 ACL

Platform description

The software version must be later than v10.0.

48.3 Security Channel

Showing and monitoring include the following commands:

- **show security** [**interface** *idx*]

Global configuration command

- **security global access-group**

Interface configuration command

- **security access-group**

- **security uplink enable**

Caution

The NPE80 does not support the security channel function.

48.3.1 show security

This command shows or specifies the security channel setting on the port.

show security [**interface** *idx*]

Parameter description

Parameter	Description
interface *idx*:	*Interface*

Command mode

Privileged mode.

Usage guidelines

This command shows the security channel setting on the specified interface. If the interface is not specified, all the security channel settings are displayed.

Examples

```
DGS-3610# show security
Port      type
-------   --------
Global     escape
Gi0/1      escape
Gi0/2      uplink
```

Related commands

Command	Function
security global access-group	Define global security channel
security access-group	Define security channel on port
security uplink enable	Specify exceptional ports in security channel

Platform description

The software version must be later than v10.2.

48.3.2 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

This command configures the global security channel.

Examples

```
DGS-3610(config)# security global access-group 1
```

Related commands

Command	Function
show security	Show the security channel setting

Platform description

The software version must be later than v10.2.

48.3.3 security access-group

This command sets 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	This command configures the security channel on the interface.
Examples	`DGS-3610(config-if)# security access-group 1`

Related commands

Command	Function
show security	Show the security channel setting.

Platform description	The software version must be later than v10.2.

48.3.4 security uplink enable

This command specifies the exceptional ports in the security channel.

security uplink enable

no security uplink enable

Parameter description	None
Command mode	Interface configuration mode.
Usage guidelines	This command specifies the exceptional ports in the security channel.
Examples	`DGS-3610(config-if)# security uplink enable`

Related commands

Command	Function
show security	Show the security channel setting

Platform description	The software version must be later than v10.2.

49 Configuring QOS Command

49.1 Default Configuration

Before configuring QoS, you must have a thorough understanding of these items related to QoS:

One interface can be associated with one policy-map at most.

One policy-map may own many class-maps

One class-map can be associated with only one ACL, and all the ACEs of this ACL must have the same filter field template.

The number of ACEs associated with an interface complies with the restriction given in "*Configuring Security ACLs*".

The QoS function is disabled by default. That is to say, the device processes all the packets in the same way. But if you associate a Policy Map with an interface and the trust mode of the interface is set,, 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 trust mode of the interface to Off. Below is the default QoS configuration:

Default CoS value	0
Number of Queues	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 mapping table from CoS value to queue

CoS Value	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Default mapping table from CoS to DSCP

CoS Value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

Default mapping table from IP-Precedence to DSCP

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default mapping table from DSCP to CoS

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

49.2 Configuration Related Commands

49.2.1 mls qos trust

Configure the QoS trust mode for an interface;

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 the default value

Default configuration

No trust.

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# mls qos trust cos
```

Related commands	**show mls qos interface** *interface-id*

49.2.2 mls qos cos

Configure the CoS value of an interface

mls qos cos *default-cos*

no mls qos cos

Parameter description

Parameter	Description
default-cos	0~7
no	Restore the default value

Default configuration	The CoS value is 0.
Command mode	Interface configuration mode.

Examples

```
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# mls qos cos 7
```

Related commands	**show mls qos interface** *interface-id*

49.2.3 Class Maps

Creat 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 See the ACL related sections

Create the class map and enter the class map configuration mode

[no] class-map *class-map-name*

Create the match standard of the class map;

[**no**] **match access-group** a*cl-name*| *acl-id*

Parameter description

Parameter	Description
acl-name	Name of the created ACL
acl-id	ID of the created ACL
class-map-name	Name of class map to be created
no class-map *class-map-name*	Delete the existing class map
no match access-group a*cl-name*| *acl-id*	Delete this match

Command mode

Global configuration mode.

Examples

Create a MAC ACL named me.

```
DGS-3610(config)# mac access-list extended me
```

Set ACL rules.

```
DGS-3610(config-ext-macl)# permit host 1111.2222.3333 any
```

Exit the ACL setting.

```
DGS-3610(config-ext-macl)# exit
```

Create the class-map and name it as cm

```
DGS-3610(config)# class-map cm
```

Associate ACLs.

```
DGS-3610(config-cmap)# match access-group me
```

Exit the class-map setting

```
DGS-3610(config-cmap)# exit
```

Related commands

show mac access-lists
show ip access-lists
show class-map

49.2.4 Policy Maps

Create the policy map and enter the policy map configuration mode

[no] policy-map *policy-map-name*

Create the class-map data classification used in the policy map and enter into the data classification configuration mode.

[no] class *class-map-name*

Set the ipdscp value of the IP messages in the dataflow, which does not take effect for non-IP messages.

set ip dscp *new-dscp*

no set ip dscp

Limit the bandwidth of the dataflow and specify the handling action for the excessive part.

police *rate-bps burst-byte*[**exceed-action** {**drop** | **dscp** *dscp-value*}]

no police

Parameter description

Parameter	Description
policy-map-name	Name of policymap 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 this data category
new-dscp	New DSCP value, whose range varies with the product
rate-bps	The limitation of bandwidth per second, in kbps
burst-byte	The burst traffic limitation, in kbyte
drop	Drop the packets of the excessive part of the bandwidth.
dscp-value	Overwrite the message DSCP value for excessive part, whose range varies with the product

Command mode

Global configuration mode.

Examples

Create a policy map and name it as "po"

```
DGS-3610(config)# policy-map po
```

Associate class-map cm

```
DGS-3610(config-pmap)# class cm
```

Set the flow dscp value as 10

	DGS-3610(config-pmap-c)# **set ip dscp** 10 Set the flow bandwidth as 1M, burst traffic as 4096k, and action for excessive part is to assign new dscp 16 DGS-3610(config-pmap-c)# **police** *1000000 4096* **exceed-action dscp** *16*
Related commands	**show policy-map**

49.2.5 service-policy

Apply policy map to the interface

service-policy {**input | output**} *policy-map-name*

no service-policy {**input | output**}

Parameter description

Parameter	Description
policy-map-name	The created name of policymap
no	Cancel the application of the policy map on the interface

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface fastEthernet 0/1
DGS-3610(config-if)# service-policy input po
```

Related commands

show mls qos interface

49.2.6 priority-queue

Configure the output queue scheduling algorithm

[n] priority-queue [**out**]

Parameter description

Parameter	Description
priority-queue [**out**]	The round robin algorithm for the output queue is SP
no priority-queue	The round robin algorithm for the output queue

	[**out**]	is WRR

Default configuration

The output queue algorithm is WRR.

Command mode

Global configuration mode.

Examples

```
DGS-3610(config)# no priority-queue out
```

Related commands

show mls qos queuing

49.2.7 war-queue bandwidth

Set the queue weight ratio of the WRR algorithm

wrr-queue bandwidth *weight1 ... weightn*

no wrr-queue bandwidth

Parameter description

Parameter	Description
weight1...weightn	*weight1...weightn* are the weight values specified for n queues output. .For the n value and its range, see the Default configuration.
no	Restore the default setting.

Default configuration

weight1: ...: weightn = 1:..:1

Command mode

Global configuration mode.

Examples

```
DGS-3610(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
```

Related commands

show mls qos queuing

49.2.8 wrr-queue cos-map

Configure the CoS value associated with the output queue

wrr-queue cos-map *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]

no wrr-queue cos-map

Parameter description

Parameter	Description
qid	Specified the queue id.
cos0 ... cos7	Associated CoS values
no	Restore the default setting

Default configuration See the default configurations

Command mode Global configuration mode.

Examples

```
DGS-3610(config)# wrr-queue cos-map 1 0 1
```

Related commands

show mls qos queuing

49.2.9 mls qos map cos-dscp

Configure the value mapped from CoS value to internal DSCP.

mls qos map cos-dscp *dscp1...dscp8*

no mls qos map cos-dscp

Parameter description

Parameter	Description
dscp	Range varies with the product
no	Restore the default setting

Default configuration See the Default configuration

Command mode

Global configuration mode.

Examples

```
DGS-3610(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 maps shows dscp-cos maps** and **ip-prec-dscp maps**

49.2.10 mls qos map dscp-cos

Configure the message internal DSCP value mapped to CoS value

mls qos map dscp-cos *dscp-list* to *cos*

no mls qos map dscp-cos

Parameter description

Parameter	Description
dscp-list	Range varies with the product
cos	Value range 0 ~ 7
no	Restore the default setting

Default configuration

See the Default configuration

Command mode

Global configuration mode.

Examples

```
DGS-3610(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

Related commands

Command	Description
show mls qos maps	Show **dscp-cos maps shows dscp-cos maps** and **ip-prec-dscp maps**

49.2.11 interface rate-limit

Configuration of port rate limitation

rate-limit {**input** | **output**} *bps burst-size*

no rate-limit

Parameter description

Parameter	Description
input	The input speed limit
output	The output speed limit
bps	Bandwidth limit per second
burst-size	Burst traffic limit (Kbyte)dscp-list, value range varying with product
no	Restore the default setting

Command mode

Interface configuration mode.

Examples

```
DGS-3610(config)# interface fastEthernet 0/1
DGS-3610(config-if)# rate-limit input 1000000 4096
```

Related commands

Command	Description
show mls qos interface	

49.2.12 mls qos scheduler

Configure the output queue scheduling algorithm

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 the default setting

Default configuration

It is the wrr scheduling by default.

Command mode	Global configuration mode.
Examples	`DGS-3610(config)# mls qos scheduler sp`
Related commands	**show mls qos scheduler**

49.2.13 drr-queue bandwidth

Set the queue weights in the DRR scheduling mode.

drr-queue bandwidth *weight1...weight8*

no drr-queue bandwidth

Parameter description

Parameter	Description
weight1...weight8	See the Default configuration for their value range
no	Restore the default setting

Default configuration	See the Default configuration
Command mode	Global configuration mode.
Examples	`DGS-3610(config)# drr-queue bandwidth 1 2 3 4 5 6 7 8`
Related commands	**show mls qos queuing**

49.2.14 mls qos map ip-prec-dscp

Configure the ippre value mapped to internal DSCP value

mls qos map ip-prec-dscp dscp1...dscp8

no mls qos map ip-prec-dscp

Parameter description

Parameter	Description
dscp	Range varies with the product
no	Restore the default setting

Default configuration

See the Default configuration

Command mode

Global configuration mode.

Examples

```
DGS-3610(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34
```

Related commands

Command	Description
show mls qos maps	Show **dscp-cos mapsshows dscp-cos maps** and **ip-prec-dscp maps**

49.2.15 wfq-queue bandwidth

When the **wfq** scheduler algorithm is used, this command configures the corresponding queues.

wfq-queue *queue-id* **bandwidth** *min max*

no wfq-queue *queue-id* **bandwidth**

Parameter description

Parameter	Description
queue-id	queue number
min	Minimum ensured bandwidth
max	Maximum allowed bandwidth

Default configuration

The **min** is the minimum port bandwidth (kbps).
The **max** is the maximum port bandwidth (kbps).

Command mode

Interface configuration mode.

Usage Guidelines

When the WFQ algorithm is used for queue scheduler, this command sets the minimum ensured bandwidth and maximum allowed bandwidth.

Examples

Set the **wfq** algorithm for queue scheduler:

```
DGS-3610(config)#  mls qos scheduler wfq
DGS-3610(config)# show mls qos scheduler
```

Configure the minimum ensured bandwidth and maximum allowed bandwidth:

```
DGS-3610(config-if)# wfq-queue 2 bandwidth 10 10240
DGS-3610(config-if)# wfq-queue 4 bandwidth 7 10240
DGS-3610(config-if)# show running
```

Related commands

Command	Description
show mls qos scheduler	Show the QOS scheduler mode

Platform description

The software version must be later than v10.1.

49.2.16 wfq-queue sp

When the WFQ scheduler algorithm is used, this command specifies whether to apply strict priority (SP) to the corresponding queues.

wfq-queue *queue-id* **sp**

no wfq-queue *queue-id* **sp**

Parameter description

Parameter	Description
queue-id	queue number
sp	SP queue scheduler algorithm

Default configuration

The sp is not used.

Command mode

Global configuration mode.

Usage Guidelines

When the WFQ algorithm is used for queue scheduler, this command enables the SP+WFQ scheduler for the queues.

Examples

Set the WFQ algorithm for queue scheduler:

```
DGS-3610(config)# mls qos scheduler wfq
DGS-3610(config)# show mls qos scheduler
```

Apply SP dispatch for queue 1 and queue 3:

```
DGS-3610(config)# wfq-queue 1 sp
DGS-3610(config)# wfq-queue 3 sp
DGS-3610(config)# show running
```

Related commands

Command	Function
show mls qos scheduler	Show the QOS scheduler mode

Platform description

The software version must be later than v10.1.

49.3 Showing Related Command

49.3.1 show class-map

Show the contents of the class map entity

show class-map [*class-map-name***]**

Parameter description

Parameter	Description
class-name	Name of class map

Default configuration

Show all class maps

Command mode

Privileged mode.

Examples

```
DGS-3610# show class-map
```

49.3.2 show policy-map

Show the contents [if the specified class class-name]of the QoS policy map entity.

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 configuration Show all policy names

Command mode Privileged mode.

Examples

```
DGS-3610# show policy-map
```

49.3.3 show mls qos interface

Use this command to display QoS configuration on the interface.

show mls qos interface [*interface-id*] [**policers**]

Parameter description

Parameter	Description
interface-id	Interface to be displayed
policers	Show the police associated with the interface

Default configuration Displaying the QoS information of all interfaces.

Command mode Privileged mode.

Examples

```
DGS-3610# show mls qos interface fastEthernet 0/1
```

49.3.4 show mls qos queuing

Show the QoS queue information (cos-to-queue map, wrr weight, drr weight)

show mls qos queueing

Command mode	Privileged mode.
Examples	`DGS-3610# show mls qos queueing`

49.3.5 show mls qos scheduler

Show the port priority queue scheduling method.

show mls qos scheduler

Command mode	Privileged mode.
Examples	`DGS-3610# show mls qos scheduler`

49.3.6 show mls qos maps

Show dscp-cos maps, dscp-cos maps and ip-prec-dscp maps

show mls qos maps [**cos-dscp | dscp-cos | ip-prec-dscp**]

Parameter description

Parameter	Description
cos-dscp	Show cos-dscp maps
dscp-cos	Show dscp-cos maps
ip-prec-dscp	Show ip-prec-dscp maps

Default configuration	Show dscp-cos maps, dscp-cos maps and ip-prec-dscp maps
Command mode	Privileged mode.
Examples	`DGS-3610# show mls qos maps`

49.3.7 show mls qos rate-limit

Show the port rate limit information

show mls qos rate-limit [**interface** *interface-id*]

Parameter description

Parameter	Description
interface	Interface where the rate-limit command is configured by interface-id.

Command mode

Privileged mode.

Examples

```
DGS-3610# show mls qos rate-limit
```

50 Configuring VRRP Command

50.1 Configuration Related Commands

The VRRP configuration commands are:

- **vrrp authentication**
- **vrrp description**
- **vrrp ip**
- **vrrp preempt**
- **vrrp priority**
- **vrrp timers advertise**
- **vrrp timers learn**
- **vrrp track**

50.1.1 vrrp authentication

This command enables the VRRP packet authentication function. The **no** format of it 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, plain text password)

Default configuration

By default, the VRRP function is not enabled on the system 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 doesn't ensure the 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
DGS-3610(config-if)# **vrrp** *group ip* *ipaddress* [**secondary**]	Enable the VRRP function set the IP address for the virtual device

50.1.2 vrrp description

This command specifies a descriptor for the VRRP. The **no** format of it restores 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 system 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 identifying 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
DGS-3610(config-if)# **vrrp** *group* ip *ipaddress* [**secondary**]	Enable the VRRP function set the IP address for the virtual device

50.1.3 vrrp ip

This command is used to enable VRRP on the interface and specify the related virtual IP address. The **no** format of the command disables the VRRP function and cancels the setting of virtual IP address.

vrrp *group* **ip** *ipaddress* [**secondary**]

no vrrp *group* **ip** *ipaddress* [**secondary**]

Parameter description

Parameter	Description
group	The VRRP group number of the virtual device
ipaddress	The IP address of the virtual device
secondary	Inidicate the secondary IP address of the virtual device

Default configuration

By default, the VRRP function is not enabled on the system interface.

Command mode

Interface configuration mode.

Usage guidelines

If the **secondary** parameter is not used, the IP address set here will become the primary IP address of the virtual device. Note that if the VRRP group is using the IP address of the Ethernet interface, to cancel the IP address of the VRRP group with the **no** command will be regarded as a configuration error by the system, because two same IP addresses are existed 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
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
DGS-3610# **show vrrp** [**brief | group**]	Show the current VRRP configuration.

50.1.4 vrrp preempt

This command sets the preemption mode of the VRRP group. The **no** command disables the VRRP preemption function.

vrrp *group* **preempt** [**delay** *seconds*]

no vrrp *group* **preempt**

Parameter description

Parameter	Description
group	VRRP group number
delay *seconds*	Optional parameter. This parameter defines the delay before a device is ready to declare its Master identity. The default value is 0s.

Default configuration

By default, the VRRP function is not enabled on the system interface. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

Command mode

Interface configuration mode.

Usage guidelines	If the VRRP group is working in the preemption mode, once a device finds its priority is higher than the Master priority, it will preempt to 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 priority, it will not preempt to 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 become the master device in the VRRP group.

Examples	In the example blow, 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
DGS-3610(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function set the IP address for the virtual device
DGS-3610(config-if)# **vrrp** *group* **priority** *level*	Set the priority for the VRRP group

50.1.5 vrrp priority

This command specifies the priority of the VRRP group. The **no** format of it restores 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 system interface. Once the VRRP function is enabled, the default priority of the VRRP group is 100.
Command mode	Interface configuration mode.

Usage guidelines

This command is used to set the VRRP group priority manually.

Examples

The example below sets the priority of VRRP group 1 as 254.

```
vrrp 1 priority 254
```

Related commands

Command	Description
DGS-3610(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device
DGS-3610(config-if)# **vrrp** *group* **preempt** [**delay** *seconds*]	Set the VRRP in the preemption mode.

50.1.6 vrrp timers advertise

This command specifies the VRRP advertising interval of the master device. The **no** format of it restores default.

vrrp *group* **timers advertise** *interval*

no vrrp *group* **timers advertise** [*interval*]

Parameter description

Parameter	Description
group	VRRP group number
interval	VRRP advertising interval (in seconds)

Default configuration

By default, the VRRP function is not enabled on the system interface. Once the VRRP function is enables, the default advertising 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 more information by sending VRRP advertisements in the set interval.

Examples

The example below sets the VRRP advertising interval as 4 seconds.

```
vrrp 1 timers advertise 4
```

Related commands

Command	Description
DGS-3610(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device
DGS-3610(config-if)# **vrrp group timers learn**	Enable the timer learning function

50.1.7 vrrp timers learn

This command enables 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 system 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 failure interval of the Master device,, 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 VRRP group 1.

```
vrrp 1 timers learn
```

Related commands

Command	Description
DGS-3610(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device
DGS-3610(config-if)# **vrrp** *group* **timers advertise** [**msec**] *interval*	Set the VRRP advertising interval

50.1.8 vrrp track

This command enables the interface monitoring function. The **no** format of it disables the function.

vrrp *group* **track** *interface-type number* [*interface -priority*]

no vrrp *group* **track** *interface-type number*

Parameter description

Parameter	Description
group	VRRP group number
interface-type	Type of monitored interface
number	Number of the monitored interface
interface-priority	VRRP priority change degree in case of the change of the monitored interface status. If not selected, the default value is 10.

Default configuration

By default, the VRRP function is not enabled on the system interface. Even if the VRRP function is enabled, no default monitored interface is specified by the system.

Command mode

Interface configuration mode.

Usage guidelines

This command can be used to monitor the outlet links. Note that the monitored interface only allows layer-3 logical interfaces to be routed (such as Routed Port, SVI, Loopback and Tunnel).

Examples

The example below enables the VRRP group 1 monitoring 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
```

Related commands

Command	Description
DGS-3610(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device
DGS-3610(config-if)# **vrrp** *group* **priority** level	Set the VRRP group priority

50.2 VRRP Monitoring and Maintenance Commands

VRRP monitoring and maintenance commands include:

- **debug vrrp**
- **debug vrrp error**
- **debug vrrp events**
- **debug vrrp packets**
- **debug vrrp state**

50.2.1 debug vrrp

This command turns on the debug switches of the VRRP error prompt, VRRP event, VRRP message and status.. The **no** format of this command disables the function.

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.

```
DGS-3610# debug vrrp
DGS-3610#
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
DGS-3610#
```

Related commands

Command	Description
DGS-3610# **debug vrrp error**	Enable the debugging switch when VRRP error prompt
DGS-3610# **debug vrrp events**	Enable the debugging switch of the VRRP event.
DGS-3610# **debug vrrp state**	Enable the debugging switch of the VRRP state.

50.2.2 debug vrrp error

This command enables the debug switches of VRRP error prompt . The **no** format of it disables the function.

debug vrrp error

no debug vrrp error

Default configuration By default, the debug switch of the VRRP error prompt is disabled.

Command mode Privileged mode.

Examples

In the example below, the user enables the debug switch of VRRP error prompt..

```
DGS-3610# debug vrrp error
DGS-3610#
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
```

50.2.3 debug vrrp events

This command enables debug switches of the VRRP event . The **no** format of it disables the function.

debug vrrp events

no debug vrrp events

Default configuration	By default, the debug switch of VRRP event is disabled.
Command mode	Privileged mode.

Examples	In the example below, the user enables the debug switch of the VRRP event.
	`DGS-3610# debug vrrp events`
	`DGS-3610#`
	`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`

50.2.4 debug vrrp packets

This command enables the debug switches of the VRRP packet . The **no** format of it disables the function.

debug vrrp packets

no debug vrrp packets

Default configuration	By default, the VRRP packet debug switch is disabled.
Command mode	Privileged mode.

Examples	In the example below, the user enables the VRRP packet debug switch, where the checksum of the packets of VRRP group 1 is displayed.
	`DGS-3610# debug vrrp packets`
	`DGS-3610#`
	`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 enables 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.
	`DGS-3610# debug vrrp packets`

```
DGS-3610#
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
```

50.2.5 debug vrrp state

This command enables the VRRP state debug switches. The **no** format of it disables the function.

debug vrrp state

no debug vrrp state

Default configuration	By default, the VRRP debug switch is enabled.
Command mode	Privileged mode.
Examples	In the example below, the user turns on the VRRP state debug switch.

```
DGS-3610# debug vrrp state
DGS-3610#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Backup -> Master
DGS-3610# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface fastethernet 0/0
DGS-3610(config-if)#no shutdown
DGS-3610(config-if)# end
DGS-3610#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Init
DGS-3610#
```

50.3 Showing Related Command

50.3.1 show vrrp

This command displays the VRRP brief or details.

show vrrp [**brief** | *group*]

Parameter description

Parameter	Description
brief	Optional parameter, showing the brief of VRRP

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:

```
DGS-3610# 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 Router 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 Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
DGS-3610#
```

Show the brief of the VRRP group:

```
DGS-3610# 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
DGS-3610#
```

Related commands

Command	Description
DGS-3610(config-if)# **vrrp** *group ip*	Enable the VRRP function and set the IP address for the virtual device

	ipaddress [**secondary**]	

50.3.2 show vrrp interface

This command shows the information of the VRRP on the specified interface.

show vrrp interface *type number* [**brief**]

Parameter description

Parameter	Description
type	Interface type
number	Interface number
brief	Optional parameter. A brief is displayed when it is used

Command mode

Privileged mode.

Examples

The example below shows the VRRP information on Ethernet interface E1/0

```
DGS-3610# 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 Router 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 Router 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
DGS-3610(config-if)# **vrrp**	Enable the VRRP function set the IP

	group **ip** *ip address* [**secondary**]	address for the virtual device

51 Configuring RLDP Command

51.1 Configuration Related Commands

The RLDP configuration commands include global configuration commands, interface mode configuration commands and privileged mode configuration commands.

The global mode configuration commands include:

- **rldp eable**
- **rldp detect-interval**
- **rldp detect-max**

The interface mode configuration commands include:

- **rldp port {unidirection-detect | bidirection-detect | loop-detect} {warning | shutdown-svi | shutdown-port | block}**
- **rldp loop-detect vlan allowed**

The privileged mode commands include:

- **rldp reset**

51.1.1 rldp enable

This command controls the global function switch of RLDP.

rldp enable

no rldp eanble

Parameter description	No parameters.
Default	Disabled
Command mode	Global configuration mode.
Usage	The port RLDP can run only when the global RLDP is enabled.

guidelines

Examples

The following example shows how to enable RLDP:

```
DGS-3610(config)# rldp enable
```

Related commands

Command	Description
rldp port	Configure the RLDP function of the port

51.1.2 rldp detect-interval

Use this command to configure the interval at which the RLDP sends detection packets on the port.

rldp detect-interval *interval*

no rldp detect-interval

Parameter description

Parameter	Description
interval	Detection interval. Value range 2-15 seconds

Default

3 seconds.

Command mode

Global configuration mode.

Usage guidelines

In the environment where STP is enabled, it is recommended that the setting interval X maximum number of detections is less than the topology convergence time of STP.

Examples

The following example shows how to set the detection interval to 5s:

```
DGS-3610(config)# rldp detect-interval 5
```

Related commands

Command	Description
rldp detect-max	Set the maximum number of detections.

51.1.3 rldp detect-max

Use this command to set the maximum number of sending detection packets on the port by RLDP. If the neighboring port does not respond when this detection number is exceeded, the link is diagnosed as faulty line.

rldp detect-max *num*

no rldp detect-max

Parameter description

Parameter	Description
num	Maximum number of detections. Value range: 2-10

Default 2.

Command mode Global configuration mode.

Usage guidelines This command is used with the detection interval to specify the maximum number of detections.

Examples The following example shows how to set the maximum number of detections to 5:

```
DGS-3610(config)# rldp detect-max 5
```

Related commands

Command	Description
Rldp detect-interval	Set the detection interval

51.1.4 rldp port

This command configures RLDP detection for the port and specifies detection type and troubleshooting method.

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	Unidirectional link detection type
bidirection-detect	Bidirectional link detection type
loop-detect	Loop detection type
warning	Warning processing

shutdown-svi	SVI where the shutdown port is located
shutdown-port	shutdown port
block	Disable the learning-forwarding function of the port

Default No default.

Command mode Interface configuration mode.

Usage guidelines The RLDP detection of the port works 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 disabling learning-forwarding of the port.

```
DGS-3610(config)# interface fas 0/1
DGS-3610(config-if)# rldp port loop-detect block
```

Related commands

Command	Description
rldp eanble	Global rldp configuration command

51.1.5 rldp loop-detect vlan allowed

This command can configure the vlan range of the loop-detection.

rldp loop-detect vlan allowed *line*

Parameter description

Parameter	Description
line	vlan access, such as: 1-4094 or 1,2,3.

Default No default.

Command mode Interface configuration mode.

Usage guidelines	Access can only detect the vlan belonging to the port. The trunk port can not detect the vlan removed.
Examples	The following example demonstrates the function of this command: `DGS-3610(config-if)# rldp loop-detect vlan allowed 1-10`

Related commands

Command	Description
rldp port	Configure the detection type of the port.

51.1.6 rldp reset

This command makes all the ports that have been processed by **rldp shutdown** or **disable** to perform rldp detection again.

rldp reset

Parameter description	No parameters.
Default	No default
Command mode	Privileged mode.
Usage guidelines	None
Examples	The example below demonstrates how to use this command: `DGS-3610# rldp reset`

Related commands

Command	Description
Rldp eanble	Rldp global configuration command

51.2 Showing and Monitoring Commands

It includes the following commands:

- **show rldp** [**interface** *intervace-id*]
- **debug rldp** {**packet | event | error**}

51.2.1 show rldp

Show the port detection information of rldp.

show rldp [**interface** *interface-id*]

Parameter description

Parameter	Description
interface-id	The port to be displayed

Command mode

Privileged EXEC configuration mode.

51.2.2 debug rldp

It is used to enable the RLDP service debugging switch. The **no** form of this command is used to disable the debugging switch.

- **debug rldp** [**packet | event | error**]
- **undebug rldp** [**packet | event | error**]

Parameter description

Parameter	Description
packet	Debugging information of receiving/sending RLDP packets.
event	Debugging information of port state change.
error	Debugging information of errors occurred during detection.

Command mode

Privileged EXEC configuration mode.

52 Configuring TPP Command

52.1 Configuration Related Commands

52.1.1 topology guard

In the global configuration command mode, use the **topology guard** command to enable the global switch of the topology protection function. Use the **no** form of this command to disable the topology protection function.

[**no**] **topology guard**

Parameter description	None
Default configuration	The topology protection function is enabled by default.
Command mode	Global configuration mode.
Usage guidelines	The topology protection function is enabled by default, so as to protect the network more effectively and prevent topology oscillation due to attack on the network. It should be used together with the **cpu topology-limit** command.

Examples	The following example shows how to enable and disable the global topology protection function:
	`DGS-3610(config)# topology guard`
	`DGS-3610(config)# no topology guard`

Related commands

Command	Description
tp-guard port enable	Enable the topology protection function for this port
cpu topology-limit	Set the CPU utilization warning

52.1.2 tp-guard port enable

Enable the topology protection function for the port. Use the **no** form of this command to disable the topology protection function for the port.

[**no**] **tp-guard port enable**

Parameter description	No parameters.
Default configuration	None.
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 the AP member port) do not support this command.

Examples	The following example shows how to configure the topology protection function for the port:
	`DGS-3610(config-if)# tp-guard port enable`
	`DGS-3610(config-if)# no tp-guard port enable`

Related commands

Command	Description
topology guard	Enable the global topology protection function

52.2 TPP Show the Command Reference

52.2.1 show tpp

Show the configuration and state of topology protection.

show tpp

Parameter description	No parameters.
Default configuration	
Command mode	Privilege 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: `DGS-3610# **show tpp**`

Related commands

Command	Description
topology guard	Enable the global topology protection function

53 Using File System Commands

53.1 Configuration Related Commands

The file system provides the following commands:

- **cat**
- **cd**
- **cp**
- **ls**
- **makefs**
- **mkdir**
- **mv**
- **pwd**
- **rm**
- **rmdir**

53.1.1 cat

This command shows the text files or binary files on the standard output device.

cat type {**bin** | **text**} **file path**

cat file path type {**bin** | **text**}

Parameter description

Parameter	Description
bin	Select the binary file to be shown.
text	Select the text file to be shown.
path	File name (including the entire path).

Default No default

Command mode Privileged mode.

Usage guidelines	This command outputs the contents of the specified file to the standard output device according to the parameters inputted on the command line. Pay attention to the following two points: a. Input of the keywords (for example, **type and file**); b. Use of the '?' help key. If you are not sure which parameter to input, you can input the "?" key to show the prompt message.

Examples	The following example is used to show the contents of the log.txt file in the tmp directory.
	`DGS-3610# cat type text file tmp/log.txt`
	The following example is used to show the contents of the tmp.bin file in the bin directory.
	`DGS-3610# cat type bin file bin/tmp.bin`

Related commands	None

53.1.2 cd

This command allows you to enter the specified directory through the directory swiching..

cd *DIRECTORY*

Parameter description

Parameter	Description
DIRECTORY	Specified directory

Default	No default
Command mode	Privileged mode.
Usage guidelines	Change the above parameter to the directory you want to enter. Use the ".." to represent the higher-level directory and the "." to represent the current-level directory. Others can be determined according to the current location. This command supports relative directories and absolute directories. After entering the specified directory, you can verity it by using the **ls** command to be described later.

Examples

Enter the tmp sub-directory of the current directory:

```
DGS-3610# cd tmp
```

Related commands

Command	Description
ls	Show the contents in the current directory

53.1.3 cp

This command allows you to copy a file to the specified file or directory.

cp dest {*DESTINE_FILE* | *DIRECTORY*} **sour** *SOURCE_FILE*

cp sour *SOURCE_FILE* **dest** {*DESTINE_FILE* | *DIRECTORY*}

Parameter description

Parameter	Description
DESTINE_FILE	Copy to a file.
DIRECTORY	File or directory to copy to.
SOURCE_FILE	Name of the file to be copied (including the path).

Default

No default.

Command mode

Privileged mode.

Usage guidelines

Copy the specified file to a new file or a directory. If the file already exists, the system will prompt whether to overwrite to cancel the operation.

Please note that the current cp command does not support the wildcard and copying of directories.

Examples

The following command copies the log.txt in the current directory to the higher-level directory:

```
DGS-3610# cp sour log.txt dest ../log_bak.txt
```

Related commands

None

53.1.4 ls

Show the information of file directories in the current directory

ls *PATHNAME*

Parameter description

Parameter	Description
PATHNAME	Optional parameter, the path of the directory to be shown, the default is the contents in the current directory

Default

By default, only the information in the current working path is shown.

Command mode

Privileged 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 current directory is shown by default.

This command does not support wildcard.

Examples

Show the information of all the files in the current directory:

```
DGS-3610# ls
```

Show the information of all the files in the tmp directory:

```
DGS-3610# ls tmp
```

Related commands

None

53.1.5 makefs

Format the device that the file system is to be mounted or the device that is to be managed by the file system

makefs dev *DEVNAME* **fs** *FSNAME*

makefs fs *FSNAME* **dev** *DEVNAME*

Parameter description

Parameter	Description
DEVNAME	Name of the device to be formatted (including the path)
FSNAME	Name of the file system to be used on the device

Default

No default

Command mode	Privileged mode.
Usage guidelines	This command is usually used in the following two cases: a. The device has never used this file system. To order to normally use the file system on the device, you need to format the device the first time . b. After the file system has been used for some time, if you want to delete all the files on the devices, you can use this command to clear all the data on the device.
Examples	See the following example: If the jffs2 is the file system to be used, and the dev/mtdblock/1 is the device to be managed by the file system: `DGS-3610# **makefs dev** */dev/mtdblock/1* **fs** *jffs2*`
Related commands	None

53.1.6 mkdir

Create directories

mkdir *DIRECTORY*

Parameter description

Parameter	Description
DIRECTORY	Name of the directory to be created.

Default	No default
Command mode	Privileged mode.
Usage guidelines	Simply enter the name of the directory you want to create (including the path). If the path contains any directory that does not exist, the creation will fail.
Examples	Create the test directory at the root directory: `DGS-3610# **mkdir** *test*`

Related commands	None

53.1.7 mv

Move the specified file to another file or directory.

mv sour *SOURCE_FILE* **dest** {*DESTINE_FILE* | *DIRECTORY*}

mv dest {*DESTINE_FILE* | *DIRECTORY*} **sour** *SOURCE_FILE*

Parameter description

Parameter	Description
SOURCE_FILE	The file to be moved.
DESTINE_FILE/DIRECTORY	The file or directory to move to

Default	No default.
Command mode	Privileged mode.
Usage guidelines	This command outputs the contents of the specified file to the standard output device according to the parameters inputted on the command line. Pay attention to the following two points: a. Input of the keywords (for example, **type** and **file**); b. Use of the '?' help key. If you are not sure which parameter to be inputted, you can press the "?" key to show the prompt message.

Examples	The following example moves the log.txt to the higher-level directory and renames it to config.txt. If a file with the same name already exists, the existing file will be replaced:
	`DGS-3610# mv sour tmp/log.txt dest ../config.txt`
	The following example moves the log.txt to the tmp directory:
	`DGS-3610# mv dest /mnt/tmp sour tmp/log.txt`

Related commands	None

53.1.8 pwd

Showing the Current Working Path

pwd

Parameter description

No parameters

Level Keyword	Description
pwd	Show the information of the current working path

Default

No default

Command mode

Privileged mode.

Usage guidelines

Show the current location.

Examples

The following example shows the current working path.

```
DGS-3610# pwd
```

Related commands

None

53.1.9 rm

Delete the specified file

rm *FILE*

Parameter description

Parameter	Description
FILE	Name of the file to be deleted (including the path).

Default

No default.

Command mode

Privileged mode.

Usage guidelines

This command does not support the wildcard, and the deletion of crossing file systems and crossing partitions. In addition, if a hard connection or symbol connection is deleted, the contents of the file

	are not affected.
Examples	Delete the log.txt file in the current directory: `DGS-3610# **rm** *log.txt*`

Related commands

Command	Description
rmdir	Delete the specified empty directory. Since the command supports abbreviations, you can use the rm command to delete directories.

53.1.10 rmdir

Deletes empty directories

rmdir *DIRECTORY*

Parameter description

Parameter	Description
DIRECTORY	Name of the directory to be deleted, which must be empty.

Default	No default.
Command mode	Privileged 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 current directory and the directory does not contain any files:
	`DGS-3610# **rmdir** *tmp*`
	`DGS-3610# **ls**`

Related commands	None

53.2 Special Notes

None

54 Configuring System Log Commands

54.1 Configuring Related Commands

54.1.1 logging on

This global command allows logs to be displayed on different devices. The **no** form of this command disables the displaying of logs.

logging on

no logging on

Parameter description	No parameters
Default configuration	Allow logs to be displayed on different devices.
Command mode	Global configuration mode.
Usage guidelines	DGS-3610 series can not only show the log information on the Console window and VTY window, but also record it in different devices such as the memory buffer, the extended FLASH and Syslog Server. This command is the main log switch. If this switch is enabled, no log will be displayed or recorded unless the log that the severity level is greater than 1.
Examples	The following example disables the log switch on the device: `DGS-3610(config)# no logging on`

Related commands

Command	Description
logging buffered	Record the Log messages to an internal buffer.

logging	Send logs to Syslog server
logging file flash:	Record log on extended FLASH
logging console	Set the level of log information that is allowed to be displayed on the console
logging monitor	Set the level of log information that is allowed to be displayed on the VTY window (such as telnet window)
logging trap	Set the level of log information that is allowed to be sent to syslog server

54.1.2 terminal monitor

This command allows log information to be displayed on the current VTY. The **no** form of this command is used to close the displaying of logs on the current VTY window.

terminal monitor

terminal no monitor

Default configuration

By default, no logs are displayed on the VTY window.

Command mode

Privileged 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 will be invalidation.

Note

For easy management, DGS-3610 series allows the use the command on the console. The **no** format 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.

```
DGS-3610# terminal monitor
DGS-3610#
```

54.1.3 logging buffered

To set the memory buffer parameters (log severity, buffer size) for logs, execute the command at the global configuration layer. The **no** format of the command disables recording logs in memory buffer.

logging buffered [*buffer-size* | *level*]

no logging buffered

Parameter description

Parameter	Description
buffer-size	Size of buffer, the value range is from 4K to 128K bytes
levelI	Severity of log, the range is from 0 to 7. The name of the severity or the numeral can be used.

Default configuration

The default buffer size is 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 the specified memory partion 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 router restart or the execution of privileged user command **clear logging**. To trace a problem, it is required to record logs in extended flash or send them to Syslog Server.

The log information of DGS-3610 series is classified into the following 8 levels:

Table 54-1

Level Keyword	Level	Description
Emergencies	**0**	**Emergency case, system cannot run normally**
Alerts	**1**	**Problems need to be correct immediate.**
Critical	**2**	**Critical conditions**
Errors	**3**	**Error message**

warnings	**4**	**Alarm information**
Notifications	**5**	**Information that is common but needs to be attentioned**
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 equals to or lower the set level will be allowed to be displayed.

Examples

The configuration example below allows logs at and lower than severity 6 to be recorded in the memory buffer with the size of 10,000 bytes.

```
DGS-3610(config)# logging buffered 10000 6
```

Related commands

Command	Description
logging on	Enable the log switch
show logging	Show the log messages in the buffer
clear logging	Clear the log messages in the log buffer

54.1.4 logging

To record the logs in the specified Syslog Sever, execute this command in the global configuration mode. To delete the specified Syslog Server in the Syslog Server list, execute the **no** format of the command.

logging *host*

no logging *host*

Parameter description

Parameter	Description
Host	Address of syslog server

Default configuration

No defaulted Syslog server.

Command mode

Global configuration mode

Usage guidelines	This command specifies a Syslog server to receive the logs of the devie. DGS-3610 series 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: `DGS-3610(config)# logging 202.101.11.1`

Related commands

Command	Description
logging on	Enable the log switch
show logging	View the log messages in buffer as well as the related log configuration parameters
logging trap	Set the level of log information that is allowed to be sent to syslog server

54.1.5 logging file flash

To store the log information in extended flash, execute the command in the global configuration mode. The **no** format of the command is used to cancel the recording log information in extended flash.

logging file flash:*filename* [*max-file-size*] [*level*]

no logging file

Parameter description

Parameter	Description
Filename	The name of the log file. without file type, fixed as the txt file
max-file-size	The maximal value of the log file. 128K ~ 6M bytes, 128K by default.
levelI	The log information level to be recorded to the log file. You can use the level name or the numeral. The defaoul log level to be written to the extended FLASH is 6. Regarding the level of log information, please refer to the Table 54-1.

Default configuration	The log information can not be recorded in the extended flash by default.
Command mode	Global configuration mode.

Usage guidelines

If no Syslog Server is specified or it is not desired to transmit logs in the network due to the consideration of security purpose, it is possible to save the logs directly in extended flash.

The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.

Caution

Extended FLASH must be purchased and installed so that the logs can be recorded in the extended FLASH. If no extended flash is installed, "**logging file flash**" is hidden automatically and cannot be configured.

Examples

The example below records the logs in extended FLASH, named trace.txt, file size 64K and log level 6.

```
DGS-3610(config)# logging file flash:trace
```

Related commands

Command	Description
logging on	Enable the log switch
show logging	View the log messages in buffer as well as the related log configuration parameters
more flash	View the logs in the extended flash

54.1.6 logging console

To set the level of logs that are allowed to be displayed on the console, execute the command in the global configuration mode. The **no** format of the command disables printing log messages on the console.

logging console *level*

no logging console

Parameter description

Parameter	Description
level	Severity of log messages, 0 ~ 7. The name of the severity or the numeral can be used. For the details of log severity, see Table 54-1.

Default configuration

Debugging (7)

Command mode	Global configuration mode.
Usage guidelines	When a log severity is set, the log messages at or lower 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 level of log that is allowed to be displayed on the console as 6: `DGS-3610(config)# logging console informational`

Related commands

Command	Description
logging on	Enable the log switch
show logging	View the log messages in buffer as well as the related log configuration parameters

54.1.7 logging monitor

To set the level of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.), execute the command in the global configuration mode. The **no** format of the command disables printing log messages on the VTY window.

logging monitor *level*

no logging monitor

Parameter description

Parameter	Description
level	Severity of the log message. The name of the level or the numeral can be used. For the details of log severity, see Table 54-1.

Default configuration	Debugging (7)
Command mode	Global configuration mode.

Usage guidelines

To print log messages on the VTY window, firstly execute 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 level of log that is allowed to be printed on the VTY window as 6:

```
DGS-3610(config)# logging monitor informational
```

Related commands

Command	Description
logging on	Enabled the log switch
show logging	View the log messages in buffer as well as the related log configuration parameters

54.1.8 logging trap

To set the level of logs that are allowed to be sent to the syslog server, execute this command in the global configuration mode. The **no** format of this command disables sending log messages to syslog server.

logging trap *level*

no logging trap

Parameter description

Parameter	Description
level	Severity of the log message. The name of the level or the numeral can be used. For the details of log severity, see Table 54-1.

Default configuration

Informational(6)

Command mode

Global configuration mode.

Usage guidelines

To send logs to the Syslog Server, firstly execute the global configuration command **logging** to configure the **Syslog Server**. Then, execute **logging trap** to specify the severity level 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 level 6 to be sent to the Syslog Server at address 202.101.11.22:

```
DGS-3610(config)# logging 202.101.11.22
DGS-3610(config)# logging trap informational
```

Related commands

Command	Description
logging on	Enable the log switch
logging	Send logs to Syslog server
show logging	View the log messages in buffer as well as the related log configuration parameters

54.1.9 logging source interface

To configure the source address of the log messages, run the command in the global configuration mode. The **no** format of the command cancels the source address setting of the message.

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

None

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 addresses.

Examples

The example below specifies loopback 0 as the source address of the syslog messages:

```
DGS-3610(config)# logging source interface loopback 0
```

Related commands

Command	Description
logging	Send logs to Syslog server

54.1.10 logging source ip

To configure the source address of the log messages, run the command in the global configuration mode. The **no** format of the command cancels the source address setting of the message.

logging source ip *A.B.C.D*

no logging source ip

Parameter description

Parameter	Description
A.B.C.D	IP addresses.

Default configuration

None

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 addresses.

Examples

The example below specifies loopback 0 as the source address of the syslog messages:

```
DGS-3610(config)# logging source ip 192.168.1.1
```

Related commands

Command	Description
logging	Send logs to Syslog server

54.1.11 logging facility

To configure the log device value, execute the command in the global configuration mode. The **no** format of the command restores the default device value (23).

logging facility *facility-type*

no logging facility

Parameter description

Parameter	Description
facility-type	Syslog device value. See the user guidelines for details.

Default configuration

Local7(23)

Command mode

Global configuration mode.

Usage guidelines

Following table is the possible device value of Syslog:

Table 2

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)

17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

The default device value is (local7) 23 by DGS-3610 series.

Examples

The example below configures the Syslog device value as **kernet**:

```
DGS-3610(config)# logging facility kern
```

Related commands

Command	Description
logging console	Set the allowed logs level to be displayed on the console.

54.1.12 logging count

To enable the log statistics function, run the following commands in the global configuration mode. To clear the log statistics data and disable the statistics function, use the **no** form of this command.

logging count

no logging count

Parameter description

No parameters.

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 cleared.

Examples	Enable the log statistics function: `DGS-3610(config)# logging count`

Related commands	**Command**	**Description**
	show logging count	Show the log information of each module in the system
	show logging	Show the basic configurations of the log module and the log information in the log buffer area.

54.1.13 service sequence-numbers

To add sequential numbers into the logs, execute the command in the global configuration mode. The **no** format of the command cancels the sequential numbers in the logs.

service sequence-numbers

no service sequence-numbers

Parameter description	None
Default configuration	No sequential number attached to the logs.
Command mode	Global configuration mode.
Usage guidelines	In addition to the timestamp, it is possible 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. `DGS-3610(config)# service sequence-numbers`

Related commands	**Command**	**Description**
	logging on	Enable the log switch
	service timestamps	Enable the timestamp in the log information

54.1.14 service timestamps

To add timestamp into the logs, execute the command in the global configuration mode. The **no** format of the command cancels the timestamps in the logs.

service timestamps *message-type* [**uptime** | **datetime**]

no service timestamps *message-type* [**uptime** | **datetime**]

default service timestamps *message-type* [**uptime | datetime**]

Parameter description

Parameter	Description
message-type	The type of log, including Log and Debug. The **log** type means the log information with severity levels 0-6. 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

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.

```
DGS-3610(config)# service timestamps debug datetime
DGS-3610(config)# service timestamps log datetime
```

Related commands

Command	Description
logging on	Enable the log switch

	service sequence-numbers	Enable the sequential number in the log information

54.1.15 service sysname

To add the sequence numbers in the logs, execute this command in the global configuration mode. The **no** form of this command cancels the sequence number in the logs.

service sysname

no service sysname

Parameter description	None
Default configuration	The log information contains no system name.
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`
	`DGS-3610#config terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`DGS-3610(config)#service sysname`
	`DGS-3610(config)#end`
	`DGS-3610#`
	`Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console`

Related commands	**Command**	**Function**
	show logging	Show the basic configurations of the log module and the log information in the log buffer area.

54.1.16 more flash

To show the contents of the log files stored in the extended FLASH, execute this command in the priviledged user mode:

more flash:*filename*

Parameter description

Parameter	Description
Filename	Log file name

Command mode

Privileged mode**.**

Usage guidelines

In the extended 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 extended FLASH as you can see:

```
DGS-3610# more  flash://f2/log.txt
look up  file in the extended flash://f2/log.txt
00004 2004-11-17 4:1:32  DGS-3610: %5:Reload requested by
Administrator. Reload Reason :Reload command
```

Related commands

Command	Function
logging file flash	Record the logs to the extended FLASH

54.1.17 clear logging

To clear the logs from the memory buffer, execute this command in the privileged user mode.

clear logging

Command mode

Privileged mode.

Usage guidelines

This command only 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.

```
DGS-3610# clear logging
```

Related commands	Command	Function
	logging on	Enable the log switch
	show logging	Show the logs in the buffer
	logging buffered	Record the logs to the memory buffer

54.2 Showing related command

54.2.1 show logging

To view the log configuration parameters and statistics of the logs and the log packets in the memory buffer, execute this command on the privileged user layer.

show logging

Parameter description	None
Command mode	Privileged mode.

Examples	The following command shows the result of the show logging command:
	`DGS-3610# **show logging**`
	`Syslog logging: enabled`
	`Console logging: level debugging, 4 messages logged`
	`Monitor logging: level informational, 0 messages logged`
	`Buffer logging: level debugging, 6 messages logged`
	`Timestamp debug messages: datetime`
	`Timestamp log messages: disabled`
	`Sequence log messages: enable`
	`Trap logging: level debugging, 2 message lines logged,0 reserved,0 fail`
	`logging to 202.101.11.22`
	`logging to 192.168.200.112`
	`Log Buffer (Total 4096 Bytes) : have written 680`
	`00001 2004-11-17 10:20:59 DGS-3610: %7:%LINK CHANGED: Interface FastEthernet 0/0, changed state to up`
	`00002 2004-11-17 10:20:59 DGS-3610: %7:%LINE PROTOCOL CHANGE: Interface FastEthernet 0/0, changed state to UP`
	`00003 2004-11-17 10:57:18 DGS-3610: %7:%LINK CHANGED: Interface FastEthernet 0/1, changed state to administratively down`
	`00004 2004-11-17 10:57:21 DGS-3610: %7:%LINK CHANGED: Interface`

```
FastEthernet 0/1, changed state to down
00005 2004-11-17 10:57:41  DGS-3610: %7:%LINK CHANGED: Interface
FastEthernet 0/1, changed state to administratively down
00006 2004-11-17 10:57:43  DGS-3610: %7:%LINK CHANGED: Interface
FastEthernet 0/1, changed state to down
```

The log messages are described as below:

Field	Description
Syslog logging	Logging flag: Displays **enabled** when it's enabled, displays **disabled** when it's 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.
Timestamp debug messages	Timestamp format of the Debug messages.
Timestamp log messages	Timestamp format of the Log messages.
Sequence log messages	Sequence flag.
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	Enable the log switch.
clear logging	Clear the logs in the buffer.

54.2.2 show logging count

To view the statistics information such as log occurrence times of the system modules and the last generation time, run the following command in the privileged mode.

show logging count

Parameter description None

Default configuration

Command mode

Privileged 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**:

```
DGS-3610# 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 basic configurations of the log module and the log information in the log buffer area
clear logging	Clear log information in log buffer area

55 Configuring POE Management Command

POE configuration management includes the following commands:

- **Poe enable/no poe enable**
- **Poe-power lower** *lower**/no poe-power lower***
- **Poe-power upper** *upper**/no poe-power upper***
- **Poe disconnect-mode** *mode***/no poe disconnect-mode**

55.1 Configuration Related Command

55.1.1 Poe enable/no poe enable

Parameter description	**None**
Command mode	Global configuration mode
Usage guidelines	This command allows you to enable/disable the remote power supply of the port.
Examples	DGS-3610(config-if)# DGS-3610(config-if)# **poe enable** DGS-3610(config-if)# **no poe enable** DGS-3610(config-if)#
Related commands	**None**

55.1.2 Poe-power lower lower/no poe-power lower

Parameter description

Parameter	Description
Lower	Indicating the minimum allowed voltage, within the range [45000-47000] mv.

Command mode

Global configuration mode.

Usage guidelines

You can use this command to set the allowed minimum voltage of the system.

Examples

The following example sets the minimum allowed voltage of the current POE system to 46000 mv.

```
DGS-3610#
DGS-3610# configure
DGS-3610(config)# poe-power lower 46000
DGS-3610(config)# end
DGS-3610#
DGS-3610#
```

Related commands

None

55.1.2.1 Poe-power upper lower/no poe-power upper

Parameter description

Parameter	Description
Upper	indicating the maximum allowed voltage, within the range [55000-57000] mv.

Command mode

Global configuration mode.

Usage guidelines

You can use this command to set the allowed maximum voltage of the system..

Examples

The following example sets the maximum allowed voltage of the current POE system to 56000 mv.

```
DGS-3610#
DGS-3610# configure
DGS-3610(config)# poe-power upper 56000
DGS-3610(config)# end
DGS-3610#
DGS-3610#
```

Related commands **None**

55.1.3 Poe disconnect-mode mode/no poe disconnect-mode

Parameter description

Parameter	Description
mode	Representing the disconnection detection mode, within the range of [ac/dc]

Command mode Global configuration mode.

Usage guidelines You can use this command to set the disconnection detection mode of the system.

Examples

Set the disconnect detection mode of the current POE system to dc:

```
DGS-3610#
DGS-3610# configure
DGS-3610(config)# poe disconnect-mode dc
DGS-3610(config)# end
DGS-3610#
DGS-3610#
```

Related commands None

55.2 Showing related command

There are the following POE showing commands:

- **show poe interfaces**
- **show poe powersupply**

55.2.1 show poe interfaces

Parameter description	None
Command mode	Privileged mode.
Usage guidelines	This command allows you to view the POE status of a port.
Examples	DGS-3610# **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 DGS-3610#

55.2.2 show poe powersupply

Parameter description	None
Command mode	Privileged mode.
Usage guidelines	This command allows you to view the POE status of a port.
Examples	DGS-3610# **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
DGS-3610#
```

56 Configuring Stack Management Command

Redundancy management includes the following related commands:

- **device-priority**
- **device-description**
- **stack on**
- **show member**

56.1 Configuration related command

56.1.1 device-priority

Command Syntax

device-priority [*member]* *priority*

Parameter description

Parameter	Description
member	Specify the member ID; It can be omitted. If omitted, it means member 1 can be configured.
priority	Priority of the member, within the range of [1, 10]

Command mode

Global configuration mode.

Usage guidelines

This command allows you to configure the stack priority of a member, within the range of 1 ~10, where 10 means the highest priority and 1 is the default value.

After setting, you must execute **write** for saving and then it will be effect.

Examples

Specify the priority of member device 2 to 8:

```
DGS-3610(config)# device-priority 2 8
```

Related commands

Command	Description
show member	Show the details of the stack member.

56.1.2 device-description

Command Syntax

device-description [member *member*] *description*

Parameter description

Parameter	Description
member *member*	Member ID; It can be omitted. If omitted, it means member 1 can be configured.
description	Descriptor of the member, with a supported length of up to 31 bytes.

Command mode

Global configuration mode.

Usage guidelines

This command allows you to set the alias of a member. After setting, you must execute **write** for saving and then it will be effect.

Examples

Specify the alias of member equipment 2 to `D-Link`:

```
DGS-3610(config)# device-description member 2 D-Link
```

Related commands

Command	Description
show member	Show the details of the stack member.

56.2 Showing related command

56.2.1 show member

Command Syntax

show member [member]

Parameter description

Parameter	Description
member	Specify the member ID. If omitted, display all the members.

Command mode

Privileged mode.

Usage guidelines

This command allows you to view the members of the stack system.

Examples

```
DGS-3610# show member
Member  Mac Address    Priority  Software Version
HardwareVersion  Description
------  --------------  -------  ---------------- --------------
---------
1       00d0.f810.3323  1       v10.1.00(2), Release(12889)  1.0
SWITCH
2       00d0.f822.33aa  1       v10.1.00(2), Release(12889)  1.0
SWITCH
3       00d0.f822.33ae  1       v10.1.00(2), Release(12889)  1.0
SWITCH
4       00d0.f822.33b0  1       v10.1.00(2), Release(12889)  1.0
SWITCH
5       00d0.f822.33b2  1       v10.1.00(2), Release(12889)  1.0
SWITCH
6       00d0.f824.23b4  1       v10.1.00(2), Release(12889)  1.0
SWITCH
7       00d0.f833.44b4  1       v10.1.00(2), Release(12889)  1.0
SWITCH
8       00d0.f855.33ae  1       v10.1.00(2), Release(12889)  1.0
SWITCH
```