

# CLI Reference Guide

---

## *Unified Services Router*

D-Link Corporation

Copyright © 2016.

<http://www.dlink.com>

---

## **CLI Reference Guide DSR-150(N) and DSR-250(N) Unified Services Router Version 3.10**

Copyright © 2016

### **Copyright Notice**

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

### **Disclaimer**

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

### **Limitations of Liability**

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

## Table of Contents

Chapter 1. Introduction .....	10
1.1 Accessing the CLI .....	10
Chapter 2. Basic commands available on the CLI.....	11
2.1 Context Sensitive Help .....	11
2.2 Auto-Completion.....	11
2.3 Movement Keys.....	11
2.4 Deletion Keys.....	11
2.5 Escape Sequences .....	12
Chapter 3. Command Hierarchy in CLI .....	13
3.1 CLI Commands.....	13
3.2 Router Configuration.....	13
Chapter 4. Global commands used in CLI .....	14
Chapter 5. Show commands used in CLI .....	15
Chapter 6. Configuration commands under branch VPN .....	45
6.1 vpn gre_tunnel add .....	45
6.2 vpn gre_tunnel edit <row_id>.....	46
6.3 vpn gre_tunnel delete <row_id>.....	46
6.4 vpn l2tp client configure.....	47
6.5 vpn l2tp client_action <action>.....	47
6.6 vpn l2tp server configure .....	47
6.7 vpn openvpn config.....	48
6.8 vpn openvpn remote_network add .....	50
6.9 vpn openvpn remote_network edit <row_id>.....	51
6.10 vpn openvpn remote_network delete <row_id>.....	51
6.11 vpn openvpn local_network add .....	51
6.12 vpn openvpn local_network edit <row_id>.....	52
6.13 vpn openvpn local_network delete <row_id>.....	52
6.14 vpn openvpn cert_upload ca <fileName> <ipAddr>.....	52
6.15 vpn openvpn cert_upload server_client_cert <fileName> <ipAddr>.....	53
6.16 vpn openvpn cert_upload client_key <fileName> <ipAddr> .....	53
6.17 vpn openvpn cert_upload dh_Key <fileName> <ipAddr>.....	53
6.18 vpn openvpn cert_upload tls_Authkey <fileName> <ipAddr> .....	53
6.19 vpn openvpn cert_upload crl_cert <fileName> <ipAddr>.....	54
6.20 vpn openvpn cert_upload config <fileName> <ipAddr> .....	54
6.21 vpn pptp client configure .....	54
6.22 vpn pptp client_action <action>.....	55
6.23 vpn pptp server configure .....	55
6.24 vpn sslvpn portal-layouts add.....	56

6.25	vpn sslvpn portal-layouts edit <row_id>.....	57
6.26	vpn sslvpn portal-layouts delete <row_id> .....	57
6.27	vpn sslvpn portforwarding appconfig add .....	58
6.28	vpn sslvpn portforwarding appconfig delete <row_id> .....	58
6.29	vpn sslvpn portforwarding hostconfig add .....	58
6.30	vpn sslvpn portforwarding hostconfig delete <row_id> .....	59
6.31	vpn sslvpn resource add .....	59
6.32	vpn sslvpn resource configure add <resource_name> .....	59
6.33	vpn sslvpn resource configure delete <row_id> .....	60
6.34	vpn sslvpn resource delete <row_id>.....	60
6.35	vpn sslvpn policy add.....	60
6.36	vpn sslvpn policy edit <row_id> .....	61
6.37	vpn sslvpn policy delete <row_id>.....	61
6.38	vpn sslvpn client .....	61
6.39	vpn sslvpn route add.....	62
6.40	vpn sslvpn route delete <row_id> .....	62
6.41	vpn ipsec policy configure <name> .....	62
6.42	vpn ipsec dhcp configure .....	70
6.43	vpn ipsec policy enable <name>.....	71
6.44	vpn ipsec policy disable <name>.....	71
6.45	vpn ipsec policy delete <name>.....	71
6.46	vpn ipsec policy connect <name>.....	71
6.47	vpn ipsec policy drop <name>.....	71
Chapter 7.	Configuration commands under branch DOT11.....	72
7.1	dot11 profile add <profile_name> .....	72
7.2	dot11 profile edit <profile_name> .....	72
7.3	dot11 radius configure .....	73
7.4	dot11 profile delete <profile_name> .....	74
7.5	dot11 accesspoint configure <ap_name>.....	74
7.6	dot11 accesspoint delete <ap_name> .....	74
7.7	dot11 accesspoint disable <ap_name> .....	75
7.8	dot11 accesspoint enable <ap_name>.....	75
7.9	dot11 radio configure .....	75
7.10	dot11 radio advanced configure.....	75
7.11	dot11 radio advanced MulToUni configure .....	76
7.12	dot11 accesspoint wps configure.....	77
7.13	dot11 accesspoint ACL configure <ap_name>.....	77
7.14	dot11 wds configure.....	77
7.15	dot11 wds mac_address add <mac_address>.....	78
7.16	dot11 wds mac_address delete <rowid>.....	78
Chapter 8.	Configuration commands under branch SYSTEM .....	79
8.1	System NT-Domain-Settings .....	79

---

8.2	system Active-Directory-Settings .....	80
8.3	system LDAP_Settings.....	81
8.4	system POP3_Settings POP3_Server_Configuration .....	82
8.5	system POP3_Settings POP3_Trusted_CA .....	83
8.6	system logging ipv4 configure .....	83
8.7	system logging facility configure <facility> .....	84
8.8	system logging remote configure .....	85
8.9	system logging ipv6 configure .....	88
8.10	system logging SMS configure.....	89
8.11	system Radius-Settings.....	89
8.12	system remote_management https configure.....	90
8.13	system remote_management telnet configure.....	91
8.14	system snmp trap configure <agent_ip>.....	91
8.15	system snmp trap delete <agent_ip> .....	92
8.16	system snmp users configure <user> .....	92
8.17	system snmp sys configure .....	93
8.18	system snmp access add.....	93
8.19	system snmp access edit <rowid>.....	94
8.20	system snmp access delete <rowid> .....	94
8.21	system switch_settings power_saving configure.....	94
8.22	system switch_settings jumbo_frame configure .....	95
8.23	system admin_setting configure .....	95
8.24	system session_setting configure.....	95
8.25	system time configure.....	96
8.26	system traffic_meter configure .....	96
8.27	system usb usb1 configure .....	97
8.28	system usb usb2 configure .....	97
8.29	system usb shareport_vlan configure <row_id> .....	98
8.30	system group add.....	98
8.31	system group edit <row_id> .....	99
8.32	system group delete <row_id> .....	100
8.33	system users add .....	100
8.34	system users edit <row_id>.....	100
8.35	system users delete <row_id>.....	101
8.36	system group groupaccesscontrol configure <group_id> .....	101
8.37	system group access_control_browser add.....	101
8.38	system group access_control_browser delete <row_id> .....	102
8.39	system group access_control_ip add .....	102
8.40	system group access_control_ip delete <row_id> .....	103
Chapter 9.	Configuration commands under branch UTIL.....	104
9.1	util system_check ping <ip_address>.....	104
9.2	util system_check dns_lookup <dns> .....	104
9.3	util system_check traceroute <ip_address>.....	104

---

9.4	util system_check capturePackets start <interface>.....	104
9.5	util system_check capturePackets download <fileName> <ipAddr>.....	104
9.6	util dbglog_download <fileName> <ipAddr> .....	104
9.7	util usb_test <ipAddr> <fileName> .....	105
9.8	util enable_auto_backup <status>.....	105
9.9	util enable_config_encryp <status>.....	105
9.10	util watchdog_disable <status>.....	105
Chapter 10. Configuration commands under branch LICENSE .....		106
10.1	license list.....	106
10.2	license activate <activationKey>.....	106
10.3	license trial_activate.....	106
10.4	license trial_activate_status.....	107
Chapter 11. Configuration commands under branch NET .....		108
11.1	net ipv6_tunnel six_to_four configure .....	108
11.2	net bandwidth profile enable <enable>.....	108
11.3	net bandwidth profile add.....	108
11.4	net bandwidth profile edit <row_id>.....	109
11.5	net bandwidth profile delete <row_id> .....	110
11.6	net bandwidth traffic_selector add.....	110
11.7	net bandwidth traffic_selector edit <row_id>.....	111
11.8	net bandwidth traffic_selector delete <row_id> .....	111
11.9	net ddns wan1 configure .....	112
11.10	net ddns wan2 configure .....	112
11.11	net ddns wan3 configure .....	113
11.12	net lan dhcp reserved_ip configure <mac_address>.....	114
11.13	net lan dhcp reserved_ip delete <mac_address> .....	115
11.14	net dmz dhcp reserved_ip configure <mac_address>.....	115
11.15	net dmz dhcp reserved_ip delete <mac_address> .....	115
11.16	net ethernet configure <interface_name>.....	115
11.17	net lan ipv4 configure.....	116
11.18	net lan ipv6 configure.....	118
11.19	net lan ipv6 pool configure <ipv6PoolStartAddr> .....	119
11.20	net lan ipv6 pool delete <ipv6PoolStartAddr>.....	120
11.21	net igmp configure.....	120
11.22	net igmp snooping configure .....	120
11.23	net igmp portmap configure <vlanId> .....	120
11.24	net intel_Amt server configure.....	121
11.25	net intel_Amt_Reflector configure.....	121
11.26	net ip_Aliasing server add.....	122
11.27	net ip_Aliasing server edit <row_id> .....	123
11.28	net ip_Aliasing server delete <row_id>.....	123
11.29	net mode configure .....	124

11.30	net ipv6_tunnel isatap add.....	124
11.31	net ipv6_tunnel isatap edit <row_id>.....	124
11.32	net ipv6_tunnel isatap delete <row_id>.....	125
11.33	net routing mode configure.....	125
11.34	net wan wan1 ipv4 configure.....	126
11.35	net wan wan2 ipv4 configure.....	137
11.36	net wan rollOverWan threeG configure.....	149
11.37	net wan mode configure.....	150
11.38	net wan port_setup configure.....	151
11.39	net wan configurable_port configure.....	151
11.40	net wan wan1 ipv6 configure.....	152
11.41	net wan wan2 ipv6 configure.....	153
11.42	16.44 net routing protocol_binding add.....	154
11.43	net routing protocol_binding edit <row_id>.....	155
11.44	net routing protocol_binding enable <row_id>.....	156
11.45	net routing protocol_binding disable <row_id>.....	156
11.46	net routing protocol_binding delete <row_id>.....	157
11.47	net radvd configure.....	158
11.48	net radvd pool add.....	159
11.49	net radvd pool edit <row_id>.....	159
11.50	net radvd pool delete <row_id>.....	160
11.51	net routing dynamic configure.....	160
11.52	net routing static ipv4 configure <name>.....	163
11.53	net routing static ipv4 edit <name>.....	163
11.54	net routing static ipv6 configure <name>.....	164
11.55	net routing static ipv6 edit <name>.....	165
11.56	net routing static ipv4 delete <name>.....	165
11.57	net routing static ipv6 delete <name>.....	166
11.58	net tahi add-default-route <ip_address>.....	166
11.59	net tahi add-route <ip_address> <gw>.....	166
11.60	net tahi del-route <ip_address> <gw>.....	166
11.61	net tahi ipv6-Alias-Add(LAN) <ip6_address>.....	166
11.62	net tahi ipv6-Alias-Del(LAN) <ip6_address>.....	167
11.63	net tahi ipv6-Alias-Add(WAN) <ip6_address>.....	167
11.64	net tahi ipv6-Alias-Del(WAN) <ip6_address>.....	167
11.65	net tahi reachable-time <time>.....	167
11.66	net tahi ping6 <ip> <size>.....	167
11.67	net tahi mping6 <mip>.....	168
11.68	net tahi bping6 <bip> <psize>.....	168
11.69	net tahi pmtu-route-add <ipAdd>.....	168
11.70	net tahi interface-down <interface>.....	168
11.71	net tahi interface-up <interface>.....	168
11.72	net tahi start-RA-custom <fileName> <ipAddr>.....	168
11.73	net tahi RA-Start.....	169

11.74	net upnp configure .....	169
11.75	net port-vlan lan_edit <portname>.....	170
11.76	net port-vlan wlan_edit <ssidName>.....	170
11.77	net vlan-membership lan_edit <portw>.....	171
11.78	net vlan-membership wlan_edit <ssidName>.....	171
11.79	net multiVlan subnet edit <vlanID>.....	172
11.80	net vlan config add <vlan_id>.....	173
11.81	net vlan config edit <vlan_id>.....	173
11.82	net vlan config delete <VlanId>.....	174
11.83	net dmz configure.....	174
Chapter 12. Configuration commands under branch SECURITY .....		176
12.1	security advanced_network attack_checks configure .....	176
12.2	security advanced_network ips setup .....	177
12.3	security application_rules add.....	177
12.4	security application_rules edit <row_id>.....	178
12.5	security application_rules delete <row_id> .....	178
12.6	security firewall custom_service add.....	179
12.7	security firewall custom_service edit <row_id>.....	179
12.8	security firewall custom_service delete <row_id>.....	180
12.9	security blocked_clients add.....	180
12.10	security blocked_clients edit <row_id> .....	181
12.11	security blocked_clients delete <row_id>.....	181
12.12	security dynamic_filter configure.....	181
12.13	security firewall ipv4 configure .....	183
12.14	security firewall ipv4 default_outbound_policy <default_outbound_policy>	185
12.15	security firewall ipv4 edit <row_id>.....	185
12.16	security firewall ipv4 enable <row_id> .....	186
12.17	security firewall ipv4 disable <row_id>.....	187
12.18	security firewall ipv4 delete <row_id> .....	187
12.19	security firewall ipv4 move <row_id> .....	187
12.20	security firewall algs.....	187
12.21	security firewall ipv6 configure .....	188
12.22	security firewall ipv6 edit <row_id>.....	189
12.23	security firewall ipv6 enable <row_id> .....	190
12.24	security firewall ipv6 disable <row_id>.....	190
12.25	security firewall ipv6 delete <row_id> .....	190
12.26	security firewall ipv6 move <row_id> .....	190
12.27	security firewall ipv6 default_outbound_policy <default_outbound_policy>	191
12.28	security ids configure .....	191
12.29	security session_settings configure .....	191
12.30	security schedules add.....	192
12.31	security schedules edit <row_id>.....	193
12.32	security schedules delete <row_id> .....	194



12.33	security firewall smtpAlg configure .....	194
12.34	security firewall smtpAlg approvedMailId add.....	194
12.35	security firewall smtpAlg approvedMailId edit <row_id> .....	195
12.36	security firewall smtpAlg approvedMailId delete <row_id>.....	195
12.37	security firewall smtpAlg blockedMailId add.....	195
12.38	security firewall smtpAlg blockedMailId edit <row_id> .....	195
12.39	security firewall smtpAlg blockedMailId delete <row_id>.....	196
12.40	security firewall smtpAlg subjectList add .....	196
12.41	security firewall smtpAlg subjectList edit <row_id>.....	196
12.42	security firewall smtpAlg subjectList delete <row_id> .....	197
12.43	security mac_filter configure .....	197
12.44	security mac_filter source add.....	197
12.45	security mac_filter source edit <row_id> .....	198
12.46	security mac_filter source delete <row_id>.....	198
12.47	security ip_or_mac_binding add .....	198
12.48	security ip_or_mac_binding edit <row_id>.....	199
12.49	security ip_or_mac_binding delete <row_id>.....	199
12.50	security firewall vpn_passthrough configure .....	199
12.51	security webAccess status <status> .....	200
12.52	security webAccess add.....	200
12.53	security webAccess edit <row_id> .....	200
12.54	security webAccess delete <row_id>.....	201
12.55	security website_filter content_filtering configure.....	201
12.56	security website_filter approved_urls add .....	201
12.57	security website_filter approved_urls edit <row_id>.....	202
12.58	security website_filter approved_urls delete <row_id>.....	202
12.59	security website_filter blocked_keywords add.....	202
12.60	security website_filter blocked_keywords edit <row_id>.....	202
12.61	security website_filter blocked_keywords delete <row_id> .....	203
12.62	security website_filter blocked_keywords enable <row_id>.....	203
12.63	security website_filter blocked_keywords disable <row_id> .....	203

# Chapter 1. Introduction

This document describes the Command Line Interface (CLI) for managing D-Link's DSR-150N / 250N router.

The CLI user requires advanced knowledge about the configuration of the system, and it should be used only by those users who are familiar with CLI-based configuration.

Note that the following features in the DSR Unified Services Router cannot be managed by the CLI:

- Firmware Upgrade
- Configuration Backup/Restore
- Certificate Generate/Upload
- Power Savings mode configuration
- System Dashboard/Resource Utilization

Please access the web browser based UI of the DSR router for managing these features.

## 1.1 Accessing the CLI

The CLI can be accessed by logging in with the same user credentials used to access the web browser based UI.

```
*****  
  
Welcome to the DSR Command Line Interface  
  
*****  
  
D-Link DSR>
```

 *D-Link DSR>* is the CLI prompt.

# Chapter 2. Basic commands available on the CLI

## 2.1 Context Sensitive Help

[?] - Displays context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.

## 2.2 Auto-Completion

The following keys both perform auto-completion for the current command line. If the command prefix is not unique a subsequent repeat of the key will display possible completions.

- [enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained.
- [space] - Auto-completes, or if the command is already resolved, inserts a space.

## 2.3 Movement Keys

- [CTRL-A] - Moves to the start of the line.
- [CTRL-E] - Moves to the end of the line.
- [up] - Moves to the previous command line held in history.
- [down] - Moves to the next command line held in history.
- [left] - Moves the insertion point left one character.
- [right] - Moves the insertion point right one character.

## 2.4 Deletion Keys

- [CTRL-C] - Deletes the whole line.
- [CTRL-D] - Deletes the character to the right on the insertion point.
- [CTRL-K] - Deletes all the characters to the right of the insertion point.
- [Backspace] - Deletes the character to the left of the insertion point.

## 2.5 Escape Sequences

- `!!` - Substitutes the last command line.
- `!N` - Substitutes the Nth command line (absolute as per 'history' command).
- `!-N` - Substitutes the command line entered N lines before (relative).

# Chapter 3. Command Hierarchy in CLI

## 3.1 CLI Commands

The CLI commands are divided into 4 categories:

- Global commands
- Show commands
- Utility commands
- Configuration commands

## 3.2 Router Configuration

The router configuration is divided into 5 branches:

- **Net:** Network Settings
- **Security:** Security Settings
- **System:** Admin Settings
- **Dot11:** Wireless Settings
- **Vpn:** VPN Settings
- **Radius:** RADIUS Settings

## Chapter 4. Global commands used in CLI

The global commands that are used in CLI are given below:

- **.exit:** Exit this session
- **.help:** Displays an overview of the CLI syntax
- **.top:** Returns to the default mode
- **.reboot:** Reboots the system.
- **.history:** Displays the current session's command line history. Number of commands in history list can be controlled by setting limit argument; by default it is unbounded.

## Chapter 5. Show commands used in CLI

The show commands for all the above mentioned branches are outlined in this section.

The command `show activeDirectory-serverCheck?` at the CLI prompt would give the description of all the show commands in the branch `activeDirectory-serverCheck`, which is as follows:

1	<code>show activeDirectory-serverCheck</code>	Displays status of Active Directory servers.
---	---	--

The command `show NT-Domain-Settings?` at the CLI prompt would give the description of all the show commands in the branch `NT-Domain-Settings`, which is as follows:

1	<code>show NT-Domain-Settings</code>	Displays NT Domain configuration.
---	--------------------------------------	-----------------------------------

The command `show vpn?` at the CLI prompt would give the description of all the show commands in the branch `vpn`, which is as follows:

1	<code>show vpn gre_tunnels</code>	<code>gre tunnels display mode</code>
2	<code>show vpn l2tp client</code>	<code>show l2tp client details</code>
3	<code>show vpn l2tp client setup</code>	Display l2tp client setup.
4	<code>show vpn l2tp client status</code>	Display l2tp client status setup.
5	<code>show vpn l2tp</code>	<code>show l2tp server details</code>
6	<code>show vpn l2tp server</code>	<code>show l2tp server details</code>
7	<code>show vpn l2tp server setup</code>	Display l2tp server setup.
8	<code>show vpn l2tp server connections</code>	Display l2tp server stats.
9	<code>show vpn openvpn</code>	Display openvpn commands
10	<code>show vpn openvpn config</code>	Display openvpn configuration
11	<code>show vpn openvpn remote_network_all</code>	Display all openvpn remote network on system
12	<code>show vpn openvpn local_network_all</code>	Display all openvpn local network on system
13	<code>show vpn openvpn cert_upload_status</code>	Display openvpn certificate status
14	<code>show vpn pptp client</code>	<code>show pptp client details</code>
15	<code>show vpn pptp client setup</code>	Display pptp client setup.
16	<code>show vpn pptp client_status</code>	<code>show pptp client status details</code>
17	<code>show vpn pptp client_status setup</code>	Display pptp client status setup.
18	<code>show vpn pptp</code>	<code>show pptp server details</code>
19	<code>show vpn pptp server</code>	<code>show pptp server details</code>
20	<code>show vpn pptp server setup</code>	Display pptp server setup.

21	show vpn pptp server connections	Display pptp server stats.
22	show vpn sslvpn	show sslvpn settings
23	show vpn sslvpn connections	show sslvpn active connections
24	show vpn sslvpn client	show sslvpn client settings
25	show vpn sslvpn route	show route settings
26	show vpn sslvpn policy	show sslvpn policy settings
27	show vpn sslvpn portal-layouts	show sslvpn portal-layouts settings
28	show vpn sslvpn portforwarding	show sslvpn portforwarding settings
29	show vpn sslvpn portforwarding appconfig	show sslvpn portforwarding appconfig settings
30	show vpn sslvpn portforwarding hostconfig	show sslvpn portforwarding hostconfig settings
31	show vpn sslvpn resource	show sslvpn resource settings
32	show vpn sslvpn resource-object <resource_name>	show sslvpn resource object settings
33	show vpn ipsec	show vpn policy
34	show vpn ipsec policy	show vpn policy
35	show vpn ipsec policy setup	show vpn policy
36	show vpn ipsec policy status	show vpn status
37	show vpn ipsec policy backup_policies	to get all list of backup policies
38	show vpn ipsec dhcp	show vpn ipsec dhcp setup
39	show vpn ipsec dhcp setup	show vpn ipsec dhcp setup

The command show LDAP-Settings? at the CLI prompt would give the description of all the show commands in the branch LDAP-Settings, which is as follows:

1	show LDAP-Settings	Displays LDAP configuration.
---	--------------------	------------------------------

The command show dot11? at the CLI prompt would give the description of all the show commands in the branch dot11, which is as follows:

1	show dot11	Display 802.11 configuration
2.	show dot11 accesspoint <ap_name>	Display Access Point configuration. This command displays the list of configured Access Points for the device. From this summary list, status and parameters of each AP are available for display. ap_name: This is an AP identifier which uniquely identifies an AP in the list of configured APs. Enabled: An AP can be disabled if not in use and enabled as needed. The AP is disabled if this field has the value 'N' and it is enabled if it has the value



	<p>'Y'. Disabling an AP does not delete the configuration, but stops the AP. Enabling the AP creates a wireless network where computers and other devices can join and communicate with the devices connected to the access point or the devices on the Local Area Network (LAN). SSID: The name or Service Set Identifier (SSID) is the name of the wireless network serviced by this AP. Note that since a given wireless profile can be common to multiple APs, the SSID is not unique to an AP. In order for computers or devices to communicate via this wireless network serviced by this AP, all devices must select the same SSID from the list of wireless networks in the area. Broadcast: The field indicates whether SSID is broadcasted or not in the beacon frames transmitted by the AP. If SSID is not broadcast, the wireless devices will not be able to see the network name (SSID). If this field has the value 'Y', it indicates that the AP's SSID is broadcasted to the public. If it is 'N' it indicates the SSID is not to be broadcasted and a device would have to specify the SSID exactly to connect to this AP. Profile: This field has a brief description of the security, encryption and authentication combination assigned to the AP. A Profile is not necessarily unique to an AP, rather this grouping of wireless settings can be used on more than one AP at the same time. Radio: The physical radio(s) on which this AP is running on. An AP can run on multiple radios at the same time for load-balancing and better throughput. VLAN: The AP can be part of a logical network defined by the VLAN id. This allows devices connected to the VLAN through this AP to exchange data with one another as in a LAN. If the optional argument <code>ap_name</code> is specified, the following configuration information is displayed for the access point. Beacon Interval: The amount of time in milliseconds between beacon transmissions. DTIM Interval: Interval for delivery of traffic indication message. It is related to beacon interval. RTS Threshold: The Request to Send (RTS) threshold is the value the AP checks against its transmitting frames to determine if the RTS/Clear To Send (CTS) handshake is required with the receiving client. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of the network packet. The default is 2346, which effectively disables RTS. Frag Threshold: This is the maximum length of the frame,</p>
--	---

		<p>beyond which packets must be broken up (fragmented) into two or more frames. Collisions occur more often for long frames because sending them occupies the channel for a longer. The default is 2346, which effectively disables Fragmentation. Preamble Mode: 802.11b requires that a preamble be prepended to every frame before it is transmitted to the air. The preamble may be either the traditional long preamble, which requires 192 microsec for transmission, or it may be an optional short preamble that requires only 96 microsec. Long preamble is needed for the compatibility with legacy 802.11 systems operating at 1 and 2 Mbps. The default is 'long'. RTS/CTS Protection: If selected the AP always performs RTS/CTS handshake before transmitting a packet. It is generally used to minimize collisions among hidden stations Transmit Power Gain: Defines the relative amplification (gain) in dbm for transmitted packets which is added to the TX power configured on the physical radio. Retry Limit: The number of retries the AP will use when a frame transmission fails. It is used for both long and short frames, of size less than or equal to the RTS threshold. Supported Rate: The rate or rates (in Mbps) which the AP will advertise in the beacon frames.</p>
3	<pre>show dot11 profile &lt;profile_name&gt; &lt;display_qos&gt;</pre>	<p>Display Profile configuration. If no profile name is specified, this command will display a summary of the details of all the profiles configured in the system. If a profile name is specified, this command will display a detailed configured of the profile. If the argument 'DisplayQosInfo' is set to 'Y', the profile details will include the QoS details as well.</p>
4	<pre>show dot11 statistics</pre>	<p>Display access point and radio statistics. This table shows a cumulative total of relevant wireless statistics for the APs and radios; the counter is reset when the device is rebooted. Radio Statistics This table displays transmit/receive data for each radio. It has the following fields: Pkt(Tx/Rx): The number of transmitted/received wireless packets Byte(Tx/Rx): The number of transmitted/received bytes of information Err(TRx/Rx): The number of transmitted/received packet errors reported to the radio Drop(Tx/Rx): The number of transmitted/received packet drops between the radio and client Mcast: The number of multicast packets sent over this radio Coll: The number of packet collisions reported to the radio AP Statistics This table displays transmit/receive data for each</p>

		AP. An AP can have multiple entries if it is running on multiple radios. It has the following fields: Pkt(Tx/Rx): The number of transmitted/received wireless packets Byte(Tx/Rx): The number of transmitted/received bytes of information Err(TRx/Rx): The number of transmitted/received packet errors reported to the AP Drop(Tx/Rx): The number of transmitted/received packet dropped by the AP Mcast: The number of multicast packets sent over this AP Coll: The number of packet collisions reported to the AP
5	show dot11 acl <ap_name>	Display access control list information for the specified access point.
6	show dot11 accesspoint status <ap_name>	Display wireless stats.
7	show dot11 radius	Display radius Information.
8	show dot11 wps	Display WPS Information.
9	show dot11 wireless_statistics	Display wireless_statistics Information.
10	show dot11 wds	Display WDS Configuration Information.
11	show dot11 radio	Display Radio configuration Available Radios This table shows the list of available radios that an AP may use. It has the following fields: Radio: The radio number. Card: This field indicates which card the radio is using. Path: This field indicates which path the radio is mapped to. RogueAP Enabled: If this field has value 'Y' it indicates that RogueAP detection is enabled on this radio. If it is 'N' it indicates that RogueAP detection is disabled on this radio. If the optional argument radioNum is given the following configuration information is displayed for the given radio. Radio Settings Radio: The radio number. Card Name: This field indicates which card the radio is using. Path: This field indicates which path the radio is mapped to. Current Channel: The channel used by the radio. RogueAP Enabled: If this field has the value 'Yes' it indicates that RogueAP detection is enabled on this radio. TX Power: Value in dBm is the default transmitted power level for all APs that use this radio. RX Diversity: Enable receive diversity (use multiple antennas to receive packets) List of Access Points for Radio This table shows all the APs that are configured for a particular radio. AP Name: This is the name of the AP. BSSID: The BSSID of the AP SSID: The SSID serviced by AP Profile: This field has a brief description of the security, encryption and authentication combination assigned to the AP.

The command show POP3-Settings? at the CLI prompt would give the description of all the show commands in the branch POP3-Settings, which is as follows:

1	show POP3-Settings	Display POP3 configuration.
---	--------------------	-----------------------------

The command show POP3-Trusted-CA? at the CLI prompt would give the description of all the show commands in the branch POP3-Trusted-CA, which is as follows:

1	show POP3-Trusted-CA	Display POP3 Trusted Certificates.
---	----------------------	------------------------------------

The command show system? at the CLI prompt would give the description of all the show commands in the branch system, which is as follows:

1	show system logging	.
2	show system logging remote	.
3	show system logging remote setup	Display remote logging configuration
4	show system logging syslogServer	.
5	show system logging syslogServer setup	Displays the syslog servers configuration
6	show system logging facility	.
7	show system logging facility setup <facility>	Display logging facility configuration
8	show system log	.
9	show system log viewLogs <facilitylevel> <categorylevel> <severitylevel>	Display viewLogs page configuration
10	show system logging ipv4	.
11	show system logging ipv4 setup	Display logging configuration
12	show system logging ipv6	.
13	show system logging ipv6 setup	Display ipv6 logs configuration
14	show system logging SMS	Display SMS logging configuration
15	show system remote_management	.
16	show system remote_management setup	Display remote management over https configuration
17	show system snmp <agentIP>	Display SNMP configuration
18	show system switch_setting	.
19	show system switch_setting power_mode	Display power mode configuration
20	show system switch_setting jumbo_frame	Display jumbo frame configuration

21	show system status	Display system status
22	show system dashboard	Displays the resources being used in the system currently
23	show system session_settings	Displays system session_settings
24	show system time	.
25	show system time setup	Display Timezone and NTP configuration
26	show system traffic_meter	.
27	show system traffic_meter setup	Display traffic meter configuration
28	show system usb	Display USB Configuration
29	show system users	System group display mode
30	show system group	System user display mode
31	show system group specific <row_id>	Display information for given group
32	show system group all	Display all groups on system
33	show system users all	Display all users on system
34	show system users specific <row_id>	Display information for given user
35	show system group groupaccesscontrol <group_id>	Displays Group Access Control configuration for the selected group
36	show system group access_control_browser	Displays Access Control browsers list
37	show system group access_control_ip	Displays Access Control ips list
38	show system firmwareVersion	Gets the firmware Version.

The command show ntDomain-serverCheck? at the CLI prompt would give the description of all the show commands in the branch ntDomain-serverCheck, which is as follows:

1	show ntDomain-serverCheck	Display status of NT Domain servers.
---	---------------------------	--------------------------------------

The command show Active-Directory-Settings? at the CLI prompt would give the description of all the show commands in the branch Active-Directory-Settings, which is as follows:

1	show Active-Directory-Settings	Display Active Directory configuration.
---	--------------------------------	---

The command show pop3-serverCheck? at the CLI prompt would give the description of all the show commands in the branch pop3-serverCheck, which is as follows:

1	show pop3-serverCheck	Display status of Pop3 servers.
---	-----------------------	---------------------------------

The command show Radius-serverCheck? at the CLI prompt would give the description of all the show commands in the branch Radius-serverCheck, which is as follows:

1	show Radius-serverCheck	Display status of Radius servers.
---	-------------------------	-----------------------------------

The command show Radius-Settings? at the CLI prompt would give the description of all the show commands in the branch Radius-Settings, which is as follows:

1	show Radius-Settings	<p>Display radius configuration.</p> <p>A RADIUS server maintains a database of user accounts used in larger environments. If a RADIUS server already exists, it can be used for authenticating users that want to connect to the wireless network provided by this device. When multiple RADIUS servers are configured they are accessed in the same order as in the table. If first RADIUS server is not accessible, then system tries to contact the next RADIUS server. Configured Radius Servers This table displays the list of all configured RADIUS servers. If the optional argument ServerIP is specified, detailed configuration of the RADIUS server is displayed.</p> <p>Server IP: IP address of RADIUS authentication server  Accounting Server IP: IP address of RADIUS accounting server  Server Port: RADIUS authentication server port to send the RADIUS messages.  Timeout: The time (in seconds) the device waits for a response from the RADIUS server  Retries: The number of tries the router will make to the RADIUS server before giving up.  Secret: RADIUS server secret. This field is only displayed if the argument ServerIP is specified.</p>
---	----------------------	--

The command show net? At the CLI prompt would give the description of all the show commands in the branch net, which is as follows:

1	show net ipv6_tunnel status	Display ipv6 tunnels status
2	show net bandwidth	.
3	show net bandwidth profile	.
4	show net bandwidth profile setup	Show list of Available Bandwidth Profile(s).
5	show net bandwidth traffic_selector	.
6	show net bandwidth traffic_selector setup	Show list of Available Traffic Selector(s).
7	show net bandwidth traffic_selector BSSID	Show list of Available BSSID(s).
8	show net bandwidth profile interface_list	Display list of interface for Inbound Bandwidth Profile.It includes Available VLANs

9	show net bandwidth traffic_selector services	Display list of available services
10	show net ddns	.
11	show net ddns setup	Show Dynamic DNS Configuration.
12	show net lan dhcp	.
13	show net lan dhcp reserved_ip	.
14	show net lan dhcp reserved_ip setup	Show list of DHCP Reserved Addresses.
15	show net lan dhcp leased_clients	.
16	show net lan dhcp leased_clients list	Show list of Available DHCP Leased Clients.
17	show net dmz	.
18	show net dmz setup	Show DMZ Configuration.
19	show net dmz dhcp	.
20	show net dmz dhcp reserved_ip	.
21	show net dmz dhcp reserved_ip setup	Show list of DMZ DHCP Reserved Addresses.
22	show net dmz dhcp leased_clients	.
23	show net dmz dhcp leased_clients list	Show list of Available DMZ DHCP Leased Clients.
24	show net ethernet	Show Ethernet interfaces
25	show net lan	.
26	show net lan ipv4	.
27	show net lan ipv4 setup	Show LAN Configuration.
28	show net lan ipv6	.
29	show net lan ipv6 setup	Show LAN Configuration.
30	show net statistics <interface>	Show Interface Statistics
31	show net igmp	Display igmp configuration
32	show net igmp snooping	Display igmp snooping configuration
33	show net intel_Amt	show IntelAmt server details
34	show net intel_Amt server	show IntelAmt Server Configurations
35	show net intel_Amt Reflector	show IntelAmt Reflector Configuration
36	show net intel_Amt server setup	Display net Intel_Amt server setup.
37	show net intel_Amt Reflector setup	Display net Intel_Amt Reflector setup.
38	show net Ip_Alias	show Ip Alias server details
39	show net Ip_Alias server	show Ip Alias configuration details
40	show net Ip_Alias server setup	Display net Intel_Amt server setup.
41	show net mode	.

42	show net mode setup	Display IP MODE configuration
43	show net ipv6_tunnel	.
44	show net ipv6_tunnel setup	Display ipv6 tunnels configuration
45	show net routing mode	.
46	show net routing mode setup	Routing Mode between WAN and LAN
47	show net wan wan1	.
48	show net wan wan1 ipv4	.
49	show net wan wan1 ipv4 status	Display ipv4 wan1 Information.
50	show net wan wan1 ipv4 setup	Display Wan1 Setup Information.
51	show net wan wan2	.
52	show net wan wan2 ipv4	.
53	show net wan wan2 ipv4 status	Display ipv4 wan2 Information.
54	show net wan wan2 ipv4 setup	Display wan2 Setup Information.
55	show net wan rollOverWan	Display the rollOverWan threeG configuration
56	show net wan rollOverWan threeG	Show rollOverWan rollOverWan threeG configuration
57	show net wan rollOverWan threeG setup	Display rollOverWan threeG Information.
58	show net wan rollOverWan threeG status	Display rollOverWan status.
59	show net wan	.
60	show net wan mode	Display wan mode Information.
61	show net wan port_setup	Display wan port Information.
62	show net wan configurable_port	Display configurable port Information.
63	show net wan wan1 ipv6	.
64	show net wan wan1 ipv6 status	Display ipv6 wan1 Information.
65	show net wan wan1 ipv6 setup	Display Wan1 Setup Information.
66	show net wan wan2 ipv6	.
67	show net wan wan2 ipv6 status	Display ipv6 wan2 Information.
68	show net wan wan2 ipv6 setup	Display Wan2 Setup Information.
69	show net routing protocol_binding	show protocol_binding rules
70	show net routing protocol_binding setup	Display protocol Binding Rules
71	show net radvd	.
72	show net radvd setup	Display RADVD configuration
73	show net routing dynamic	Show dynamic routing setup
74	show net routing dynamic setup	Show dynamic routing Setup.



75	show net routing	Displays routing setup
76	show net routing static	.
77	show net routing static ipv4	.
78	show net routing static ipv4 setup	Show all the configured IPV4 routes.
79	show net routing static interface_list	Show all the interfaces on which static route can be configured
80	show net routing static ipv6	.
81	show net routing static ipv6 setup	Show all the configured IPV6 routes.
82	show net upnp	Display UPnP Information
83	show net upnp portmap	Display UPnP portmap Information.
84	show net upnp setup	Display UPnP portmap Information.
85	show net vlan	
86	show net vlan configuration	
87	show net multivlan	show vlan server status
88	show net multivlan subnet	show vlan server status
89	show net multivlan subnet status	Display vlan server status.
90	show net port-vlan	show Port vlan status
91	show net port-vlan status	Display Port vlan status.
92	show net wireless_vlan	show Port vlan status
93	show net wireless_vlan status	Display Port vlan status.

The command show ldap-serverCheck? at the CLI prompt would give the description of all the show commands in the branch ldap-serverCheck, which is as follows:

1	show ldap-serverCheck	Display status of Ldap servers.
---	-----------------------	---------------------------------

The command show security? at the CLI prompt would give the description of all the show commands in the branch security, which is as follows:

1	show security advanced_network	show advanced firewall attack checks
2	show security advanced_network attack_checks	Display Security Checks configuration
3	show security advanced_network ips	Display ips configuration
4	show security application_rules	.
5	show security application_rules setup	Display application rules configuration
6	show security application_rules status	Display application rules status

7	show security firewall custom_service	.
8	show security firewall custom_service setup	Display Custom Service configuration
9	show security blocked_clients	.
10	show security blocked_clients setup	Display Blocked Clients configuration
11	show security dynamic_filter	show dynamic filtering configuration setup.
12	show security dynamic_filter configuration	
13	show security firewall	Display Firewall Rules
14	show security firewall ipv4	Display Firewall Rules
15	show security firewall ipv4 setup	Display Firewall Rules
16	show security firewall algs	Display ALGs protocols status
17	show security firewall ipv6	Display IPV6 Firewall Rules
18	show security firewall ipv6 setup	Display Firewall Rules
19	show security ids	.
20	show security ids setup	Display IDS configuration
21	show security session_settings	Display Session Settings configuration
22	show security schedules	.
23	show security schedules setup	Display Schedules configuration
24	show security firewall smtpAlg	.
25	show security firewall smtpAlg configure	.
26	show security firewall smtpAlg configure setup	Show SmtplAlg Status.
27	show security firewall smtpAlg approvedMailld	.
28	show security firewall smtpAlg approvedMailld setup	Show List of Approved Mail_Id.
29	show security firewall smtpAlg blockedMailld	.
30	show security firewall smtpAlg blockedMailld setup	Show List of Blocked Mail_Id.
31	show security firewall smtpAlg subjectList	.
32	show security firewall smtpAlg subjectList setup	Show List of Subject, Mail_Id, Action.
33	show security mac_filter	.
34	show security mac_filter setup	Display Source Mac Filter configuration
35	show security ip_or_mac_binding	.

36	show security ip_or_mac_binding setup	Display IP/MAC Binding configuration
37	show security firewall vpn_passthrough	.
38	show security firewall vpn_passthrough setup	Display VPN passthrough Configuration
39	show security webAccess	.
40	show security webAccess setup	Display security webAccess rules
41	show security website_filter	.
42	show security website_filter content_filtering	Display content filtering configuration
43	show security website_filter approved_urls	Display trusted domains configuration
44	show security website_filter blocked_keywords	Display blocked keywords configuration

The command `vpn?` at the CLI prompt would give the description of all the configuration commands in the branch `vpn`, which is as follows:

1	vpn gre_tunnel	GRE Tunnel.
2	vpn gre_tunnel add	GRE Tunnel configuration mode
3	vpn gre_tunnel edit <row_id>	GRE Tunnel configuration mode
4	vpn gre_tunnel delete <row_id>	GRE Tunnel delete mode
5	vpn l2tp client	vpn policy mode.
6	vpn l2tp client configure	l2tp client configuration mode
7	vpn l2tp client_action <action>	vpn l2tp client action set.
8	vpn l2tp	vpn policy mode.
9	vpn l2tp server	vpn policy mode.
10	vpn l2tp server configure	l2tp server configuration mode
11	vpn openvpn	Display openvpn configure commands
12	vpn openvpn config	openvpn configuration mode
13	vpn openvpn remote_network	open vpn remote networks configuration commands.
14	vpn openvpn remote_network add	add a new remote network
15	vpn openvpn remote_network edit <row_id>	remote network edit mode.
16	vpn openvpn remote_network delete <row_id>	openvpn remote network delete mode.
17	vpn openvpn local_network	open vpn local networks configuration commands.
18	vpn openvpn local_network add	add a new local network

19	vpn openvpn local_network edit <row_id>	local network edit mode.
20	vpn openvpn local_network delete <row_id>	openvpn local network delete mode.
21	vpn openvpn cert_upload	openvpn local network display mode
22	vpn openvpn cert_upload ca <fileName> <ipAddr>	upload the pem formatted CA Certificate
23	vpn openvpn cert_upload server_client_cert <fileName> <ipAddr>	upload the pem formatted Server / Client Certificate
24	vpn openvpn cert_upload client_key <fileName> <ipAddr>	upload the pem formatted Server/Client key
25	vpn openvpn cert_upload dh_Key <fileName> <ipAddr>	upload the pem formatted Diffie Hellman key
26	vpn openvpn cert_upload tls_Authkey <fileName> <ipAddr>	upload the pem formatted Tls Authentication Key
27	vpn openvpn cert_upload crl_cert <fileName> <ipAddr>	upload the pem formatted CRL Certificate
28	vpn openvpn cert_upload config <fileName> <ipAddr>	upload the pem formatted config file
29	vpn pptp client	vpn policy mode.
30	vpn pptp client configure	pptp client configuration mode
31	vpn pptp client_action <action>	vpn pptp client action set.
32	vpn pptp	vpn policy mode.
33	vpn pptp server	vpn policy mode.
34	vpn pptp server configure	pptp server configuration mode
35	vpn sslvpn	sslvpn configuration commands
36	vpn sslvpn portal-layouts	sslvpn portal layout configuration commands
37	vpn sslvpn portal-layouts add	Add sslvpn portal layout
38	vpn sslvpn portal-layouts edit <row_id>	Edit sslvpn portal layout
39	vpn sslvpn portal-layouts delete <row_id>	Delete sslvpn portal layout
40	vpn sslvpn portforwarding	sslvpn portforwarding configuration commands
41	vpn sslvpn portforwarding appconfig	sslvpn portforwarding application configuration commands
42	vpn sslvpn portforwarding appconfig add	Add an application configuration rule

43	vpn sslvpn portforwarding appconfig delete <row_id>	Delete an application configuration rule
44	vpn sslvpn portforwarding hostconfig	sslvpn portforwarding host configuration commands
45	vpn sslvpn portforwarding hostconfig add	Add a host configuration rule
46	vpn sslvpn portforwarding hostconfig delete <row_id>	Delete a host configuration rule
47	vpn sslvpn resource	sslvpn resource configuration commands
48	vpn sslvpn resource add	Add an sslvpn resource
49	vpn sslvpn resource configure	Configure an sslvpn resource
50	vpn sslvpn resource configure add <resource_name>	Add an sslvpn resource object
51	vpn sslvpn resource configure delete <row_id>	Delete an sslvpn resource object
52	vpn sslvpn resource delete <row_id>	Delete an sslvpn resource
53	vpn sslvpn policy	sslvpn policy configuration commands
54	vpn sslvpn policy add	Add an sslvpn policy
55	vpn sslvpn policy edit <row_id>	Edit an sslvpn policy
56	vpn sslvpn policy delete <row_id>	Delete an sslvpn policy
57	vpn sslvpn client	sslvpn client configuration commands
58	vpn sslvpn route	sslvpn route configuration commands
59	vpn sslvpn route add	Add sslvpn client route
60	vpn sslvpn route delete <row_id>	Delete sslvpn client route
61	vpn ipsec	vpn policy mode.
62	vpn ipsec policy	vpn policy mode.
63	vpn ipsec policy configure <name>	vpn policy configuration mode
64	vpn ipsec dhcp	vpn ipsec over dhcp mode.
65	vpn ipsec dhcp configure	vpn dhc/ over ipsecpolicy configuration mode
66	vpn ipsec policy enable <name>	enable a vpn policy
67	vpn ipsec policy disable <name>	disable a vpn policy
68	vpn ipsec policy delete <name>	delete a vpn policy
69	vpn ipsec policy connect <name>	connect a vpn tunnel
70	vpn ipsec policy drop <name>	drop a vpn tunnel

The command `dot11?` at the CLI prompt would give the description of all the configuration commands in the branch `dot11`, which is as follows:

1	<code>dot11 profile</code>	802.11 profile configuration.
2	<code>dot11 accesspoint</code>	802.11 access point configuration.
3	<code>dot11 radio</code>	802.11 radio configuration.
4	<code>dot11 radius</code>	802.11 radius configuration mode.
5	<code>dot11 wds</code>	802.11 wds configuration.
6	<code>dot11 wds mac_address</code>	802.11 wds mac_address configuration.
7	<code>dot11 profile add &lt;profile_name&gt;</code>	802.11 profile configuration mode.
8	<code>dot11 profile edit &lt;profile_name&gt;</code>	802.11 profile configuration mode.
9	<code>dot11 radius configure</code>	802.11 radius configuration mode.
10	<code>dot11 profile delete &lt;profile_name&gt;</code>	Delete an 802.11 profile.
11	<code>dot11 accesspoint configure &lt;ap_name&gt;</code>	802.11 access point configuration mode
12	<code>dot11 accesspoint delete &lt;ap_name&gt;</code>	Delete an 802.11 access point.
13	<code>dot11 accesspoint disable &lt;ap_name&gt;</code>	Disable an 802.11 access point.
14	<code>dot11 accesspoint enable &lt;ap_name&gt;</code>	Enable an 802.11 access point.
15	<code>dot11 radio configure</code>	802.11 radio configuration mode.
16	<code>dot11 radio advanced</code>	Advanced radio configure
17	<code>dot11 radio advanced configure</code>	802.11 AP advanced configuration mode.
18	<code>dot11 radio advanced MulToUni</code>	Advanced radio configure
19	<code>dot11 radio advanced MulToUni configure</code>	802.11 AP advanced configuration mode.
20	<code>dot11 accesspoint wps</code>	Advanced AP configure
21	<code>dot11 accesspoint wps configure</code>	802.11 AP wps configuration mode.
22	<code>dot11 accesspoint acl</code>	Accesspoint ACL configure
23	<code>dot11 accesspoint ACL configure &lt;ap_name&gt;</code>	802.11 AP ACL configuration mode.
24	<code>dot11 wds configure</code>	wds configuration mode.
25	<code>dot11 wds mac_address add &lt;mac_address&gt;</code>	add wds peer mac address.
26	<code>dot11 wds mac_address delete &lt;rowid&gt;</code>	delete the wds peer mac_address.

27	dot11 wds mac_address deleteAll	delete all the wds peer mac_addresses.
----	------------------------------------	--

The command system? at the CLI prompt would give the description of all the configuration commands in the branch system, which is as follows:

1	system POP3_Settings	System POP3 configuration commands.
2	system NT-Domain-Settings	Configure NT-Domain Settings
3	system Active-Directory-Settings	Configure Active-Directory Settings
4	system LDAP_Settings	Configure LDAP Settings
5	system POP3_Settings POP3_Server_Configuration	Configure POP3 Server
6	system POP3_Settings POP3_Trusted_CA	Upload POP3 trusted Certificates
7	system logging	.
8	system logging ipv4	System logging configuration.
9	system logging facility	System log Facility configuration.
10	system logging facility Options	System log Facility configuration.
11	system logging remote	System remoteLogging configuration.
12	system logging ipv6	System ipv6 logs configuration.
13	system logging SMS	System SMS logs configuration.
14	system logging ipv4 configure	System logging configuration mode.
15	system logging facility configure <facility>	System logging facility configuration mode.
16	system logging remote configure	System remote Logging configuration mode.
17	system logging ipv6 configure	System ipv6 logs configuration mode.
18	system logging SMS configure	System SMS logging configuration mode
19	system Radius-Settings	Configure Radius-Settings.
20	system remote_management	Remote Mgmt Setup.
21	system remote_management https	Remote Mgmt Setup for https.
22	system remote_management https configure	Configure remote management support for https.
23	system remote_management telnet configure	Configure remote management support for telnet.
24	system snmp	System SNMP configuration.
25	system snmp trap	System SNMP trap configuration.
26	system snmp sys	System SNMP system configuration.
27	system snmp access	System SNMP Access Configuration.
28	system snmp users	System SNMP v3 User Configuration.
29	system snmp trap configure	SNMP trap configuration mode.

	<agent_ip>	
30	system snmp trap delete <agent_ip>	Delete a SNMP trap configuration.
31	system snmp users configure <user>	SNMP v3 User list configuration changes
32	system snmp sys configure	SNMP system configuration mode
33	system snmp access add	snmp access configuration mode
34	system snmp access edit <rowid>	snmp configuration mode
35	system snmp access delete <rowid>	snmp access configuration mode
36	system switch_settings	switch setting setup.
37	system switch_settings power_saving	power saving setup.
38	system switch_settings jumbo_frame	jumbo frame setup.
39	system switch_settings power_saving configure	power saving configuration mode.
40	system switch_settings jumbo_frame configure	jumbo frame configuration mode.
41	system admin_setting	System configuration.
42	system admin_setting configure	System configuration mode.
43	system session_setting	System session settings configuration.
44	system session_setting configure	User session configuration mode.
45	system time	System time configuration mode
46	system time configure	System time configuration mode
47	system traffic_meter	traffic meter Configuration setup.
48	system traffic_meter configure	traffic meter configuration mode.
49	system usb	USB Configuration.
50	system usb usb1	USB1 Configuration.
51	system usb usb1 configure	USB1 Configuration.
52	system usb safelyRemoveUsb	safely removing the USB.
53	system usb SafelyRemoveUSB usb1	To Unmount usb1
54	system usb SafelyRemoveUSB usb2	To Unmount usb2
55	system usb usb2	USB2 Configuration.
56	system usb usb2 configure	USB2 Configuration.
57	system usb shareport_vlan	USB SharePort settings.
58	system usb shareport_vlan configure <row_id>	SharePort on vlan configuration.



59	system usb shareport_vlan show	SharePort on vlan status.
60	system users	System user configuration commands.
61	system group	System group configuration commands.
62	system group add	system groups add mode.
63	system group edit <row_id>	system groups edit mode.
64	system group delete <row_id>	system groups delete mode.
65	system users add	system users add mode.
66	system users edit <row_id>	system users edit mode.
67	system users delete <row_id>	system users delete mode.
68	system group groupaccesscontrol	group access control
69	system group groupaccesscontrol configure <group_id>	group access control configuration
70	system group access_control_browser	List of browsers for which login policies can be applied
71	system group access_control_browser add	Add a browser to Access Control browsers list
72	system group access_control_browser delete <row_id>	Delete a browser from Access Control browsers list
73	system group access_control_ip	List of ips for which login policies can be applied
74	system group access_control_ip add	Add an ip to Access Control ips list
75	system group access_control_ip delete <row_id>	Delete an ip from Access Control ips list

The command `util ?` at the CLI prompt would give the description of all the configuration commands in the branch `util` , which is as follows:

1	util restore-factory-defaults	Revert to factory default settings.
2	util system_check	system check options
3	util system_check ping <ip_address>	Ping an Internet Address.
4	util system_check dns_lookup <dns>	To retrieve the IP address of a Web, FTP, Mail or any other Server on the Internet
5	util system_check traceroute <ip_address>	display all the routers present between the destination IP address and this router
6	util system_check display_IPV4_routingtable	Display IPV4 Routing Table

7	util system_check display_IPV6_routingtable	Display IPV6 Routing Table
8	util system_check capturePackets	Allows you to capture all packets that pass through the selected interface
9	util system_check capturePackets start <interface>	Start the packet capture
10	util system_check capturePackets avail_interfaces	Display available interfaces for packet capture
11	util system_check capturePackets stop	Stop the packet capture
12	util system_check capturePackets download <fileName> <ipAddr>	Download the packet capture to the host machine
13	util dbglog_download <fileName> <ipAddr>	Download Dbglogs to the host machine
14	util reboot	Reboot the system.
15	util usb_test <ipAddr> <fileName>	To test the USB.
16	util enable_auto_backup <status>	Enable/Disable Auto Backup support
17	util enable_config_encryp <status>	Enable/Disable Configuration encryption support
18	util watchdog_disable <status>	Disable/Enable watchdog timer

The command license? at the CLI prompt would give the description of all the configuration commands in the branch license, which is as follows:

1	license list	List license on the device
2	license activate <activationKey>	activate a license on the device.
3	license trial_activate	Activate trial period of 90 days to use WCF.
4	license trial_activate_status	displays the details of free trial expiry in days.

The command net? at the CLI prompt would give the description of all the configuration commands in the branch net, which is as follows:

1	net ipv6_tunnel	ipv6 tunnel configuration setup.
2	net ipv6_tunnel six_to_four	six to four tunnel configuration setup.
3	net ipv6_tunnel six_to_four configure	six To Four Tunnel configuration mode.
4	net bandwidth	.
5	net bandwidth profile	It gives options to add/edit/delete a bandwidth profile.

6	net bandwidth profile enable <enable>	It allows to enable/disable bandwidth profiles.
7	net bandwidth profile add	It allows to add a bandwidth profile.
8	net bandwidth profile edit <row_id>	It allows to edit a bandwidth profile.
9	net bandwidth profile delete <row_id>	It allows to delete a bandwidth profile.
10	net bandwidth traffic_selector	It gives options to add/edit/delete a traffic selector for a bandwidth profile.
11	net bandwidth traffic_selector add	It allows to add a traffic selector for a bandwidth profile.
12	net bandwidth traffic_selector edit <row_id>	It allows to edit a traffic selector for a bandwidth profile.
13	net bandwidth traffic_selector delete <row_id>	It allows to delete a traffic selector for a bandwidth profile.
14	net ddns	DDNS setup.
15	net ddns wan1	DDNS setup.
16	net ddns wan2	DDNS setup.
17	net ddns wan3	DDNS setup.
18	net ddns wan1 configure	DDNS configuration mode.
19	net ddns wan2 configure	DDNS configuration mode.
20	net ddns wan3 configure	DDNS configuration mode.
21	net lan dhcp	DHCP setup.
22	net lan dhcp reserved_ip	DHCP Reserved IPs setup.
23	net lan dhcp reserved_ip configure <mac_address>	DHCP Reserved IPs add/edit mode.
24	net lan dhcp reserved_ip delete <mac_address>	Delete a specific reserved ip entry.
25	net dmz dhcp	DHCP setup.
26	net dmz dhcp reserved_ip	DHCP Reserved IPs setup.
27	net dmz dhcp reserved_ip configure <mac_address>	DHCP Reserved IPs add/edit mode.
28	net dmz dhcp reserved_ip delete <mac_address>	Delete a specific reserved ip entry.
29	net ethernet	Ethernet configuration.
30	net ethernet configure <interface_name>	Ethernet configuration mode.
31	net lan	LAN setup.
32	net lan ipv4	.
33	net lan ipv4 configure	IPv4 LAN configuration mode.
34	net lan ipv6	.
35	net lan ipv6 configure	IPv6 LAN configuration mode.

36	net lan ipv6 pool	.
37	net lan ipv6 pool configure <ipv6PoolStartAddr>	IPv6 LAN configuration add/edit mode.
38	net lan ipv6 pool delete <ipv6PoolStartAddr>	IPv6 LAN configuration delete.
39	net igmp	igmp configuration commands
40	net igmp configure	Specify igmp proxy should be enable or disable
41	net igmp snooping	igmp snooping configuration commands
42	net igmp snooping configure	Specify igmp snooping should be enable or disable
43	net igmp portmap	igmp snooping portmap configuration commands
44	net igmp portmap configure <vlanId>	Specify igmp port map configuration
45	net intel_Amt	net policy mode.
46	net intel_Amt server	net policy mode.
47	net intel_Amt server configure	Intel Amt server configuration mode
48	net intel_Amt_Reflector	net policy mode.
49	net intel_Amt_Reflector configure	Intel Amt Reflector configuration mode
50	net ip_Aliasing	net policy mode.
51	net ip_Aliasing server	net policy mode.
52	net ip_Aliasing server add	Ip Aliasing server configuration
53	net ip_Aliasing server edit <row_id>	Editing Ip Aliasing server configuration.
54	net ip_Aliasing server delete <row_id>	Delete Ip Aliasing configuratio
55	net mode	IP Mode Setup
56	net mode configure	IP Mode configuration mode.
57	net ipv6_tunnel isatap	isatap tunnel configuration setup.
58	net ipv6_tunnel isatap add	isatap tunnel configuration mode.
59	net ipv6_tunnel isatap edit <row_id>	isatap Tunnel configuration mode.
60	net ipv6_tunnel isatap delete <row_id>	isatap tunnel configuration mode.
61	net routing mode	Routing Mode between WAN and LAN setup.
62	net routing mode configure	Routing Mode between WAN and LAN configuration mode.
63	net wan wan1	wan configuration mode
64	net wan wan1 ipv4	ipv4 wan configuration mode
65	net wan wan1 ipv4 configure	ipv4 wan wan1 configuration mode
66	net wan wan2	wan configuration mode
67	net wan wan2 ipv4	ipv4 wan configuration mode
68	net wan wan2 ipv4 configure	ipv4 wan wan2 configuration mode
69	net wan rollOverWan	rollOverWan threeG configuration mode
70	net wan rollOverWan threeG	rollOverWan threeG configuration mode

71	net wan rollOverWan threeG configure	rollOverWan threeG configuration mode
72	net wan	wan mode configuration mode
73	net wan mode	wan mode configuration mode
74	net wan mode configure	wan mode configuration mode
75	net wan port_setup	wan port setup.
76	net wan port_setup configure	wan port configuration mode.
77	net wan configurable_port	configurable port setup.
78	net wan configurable_port configure	configurable port setup.
79	net wan wan1 ipv6	ipv6 wan configuration mode
80	net wan wan1 ipv6 configure	ipv6 wan1 configuration mode
81	net wan wan2 ipv6	ipv6 wan2 configuration mode
82	net wan wan2 ipv6 configure	ipv6 wan2 configuration mode
83	net routing protocol_binding	protocol_binding rules
84	net routing protocol_binding add	protocol_binding rules configuration mode.
85	net routing protocol_binding edit <row_id>	protocol_binding rules configuration mode.
86	net routing protocol_binding enable <row_id>	protocol_binding rules configuration mode.
87	net routing protocol_binding disable <row_id>	protocol_binding rules configuration mode.
88	net routing protocol_binding delete <row_id>	protocol_binding rules configuration mode.
89	net radvd	RADVD configuration setup.
90	net radvd pool	RADVD configuration setup.
91	net radvd configure	radvd configuration mode.
92	net radvd pool add	radvd Pool configuration mode.
93	net radvd pool edit <row_id>	radvd Pool configuration mode.
94	net radvd pool delete <row_id>	radvd pool configuration mode.
95	net routing dynamic	Configure the routes dynamically.
96	net routing dynamic configure	configure the routes dynamically.
97	net routing	configure routing mode, static and dynamic route(s).
98	net routing static	Configure the routes.
99	net routing static ipv4	Configure the routes.
100	net routing static ipv6	Configure the IPV6 routes.
101	net routing static ipv4 configure <name>	Add new static routes.
102	net routing static ipv4 edit <name>	Edit existing static routes.

103	net routing static ipv6 configure <name>	Add new IPV6 static routes.
104	net routing static ipv6 edit <name>	Edit existing IPV6 static routes.
105	net routing static ipv4 delete <name>	Delete a specific route.
106	net routing static ipv6 delete <name>	Delete a specific IPV6 route.
107	net routing static ipv4 deleteAll	Delete all the configured routes.
108	net routing static ipv6 deleteAll	Delete all the configured IPV6 routes.
109	net tahi	settings for tahi test suite.
110	net tahi add-default-route <ip_address>	add ipv6 default route on lan interface.
111	net tahi delete-default-route	delete ipv6 default route on lan interface.
112	net tahi add-route <ip_address> <gw>	add ipv6 route on lan interface.
113	net tahi del-route <ip_address> <gw>	add ipv6 route on lan interface.
114	net tahi stop-RA	stop sending RA.
115	net tahi start-RA- AdvRetransTimer(1000)	start sending RA with AdvRetransTimer as 1000.
116	net tahi start-RA- AdvRetransTimer(5000)	start sending RA with AdvRetransTimer as 5000.
117	net tahi startRA- Reachable(30000)Retrans(1000)	start sending RA with AdvReachableTime as 30000 and AdvRetransTimer as 1000.
118	net tahi start-RA- AdvReachableTime(10000)	start sending RA with AdvReachableTime as 10000.
119	net tahi start-RA- AdvReachableTime(30000)	start sending RA with AdvReachableTime as 30000.
120	net tahi start-RA(Default)	start sending RA with default parameters.
121	net tahi start-RA-MinValues	start sending RA with minimum values of parameters.
122	net tahi start-RA-MaxValues	start sending RA with maximum values of parameters.
123	net tahi start-RA- MaxRtrAdvInterval(10)	start sending RA with MaxRtrAdvInterval value of 10.
124	net tahi start-RA- MaxRtrAdvInterval(40)	start sending RA with MaxRtrAdvInterval value of 40.
125	net tahi start-RA- MinRtrAdvInterval(198)	start sending RA with MinRtrAdvInterval value of 198.
126	net tahi start-RA-prefix(8000::)	start sending RA with prefix 8000::/64.

127	net tahi start-RA-prefix(fec0::)	start sending RA with prefix fec0::/64.
128	net tahi start-RA-AdvCurHopLimit(0)	start sending RA with AdvCurHopLimit value as 0.
129	net tahi start-RA-AdvCurHopLimit(15)	start sending RA with AdvCurHopLimit value as 15.
130	net tahi start-RA-WAN	start sending RA on the WAN interface.
131	net tahi ipv6-down	disable the ipv6 stack on the router.
132	net tahi ipv6-up	enable the ipv6 stack on the router.
133	net tahi ipv6-global-up	enable the ipv6 stack on the router and adds global ip.
134	net tahi ipv6-Alias-Add(LAN) <ip6_address>	Add ipv6 address to LAN interface.
135	net tahi ipv6-Alias-Del(LAN) <ip6_address>	Delete an ipv6 address from LAN interface.
136	net tahi ipv6-Alias-Add(WAN) <ip6_address>	Add ipv6 address to WAN interface.
137	net tahi ipv6-Alias-Del(WAN) <ip6_address>	Delete an ipv6 address from WAN interface.
138	net tahi neigh-cache-del	deletes the ipv6 neighbor cache.
139	net tahi reachable-time <time>	set the reachable time of neighbour cache entries
140	net tahi mcast-start	start ipv6 multicast
141	net tahi mcast-stop	stop ipv6 multicast
142	net tahi ping6 <ip> <size>	ping6 on LAN interface with count one
143	net tahi mping6 <mip>	multicast ping6 on LAN
144	net tahi bping6 <bip> <psize>	ping6
145	net tahi pmtu-route-add <ipAddr>	add ipv6 route on lan interface.
146	net tahi disable-ipv6-firewall	disable ipv6 firewall.
147	net tahi show-LAN-ip	show ipv6 addresses of LAN interface.
148	net tahi interface-down <interface>	brings selected interface down.
149	net tahi interface-up <interface>	brings selected interface up.
150	net tahi start-RA-custom <fileName> <ipAddr>	starts RA with configuration file obtained through tftp.
151	net tahi RA-Start	starts RA with custom configuration.
152	net upnp	Upnp configuration mode
153	net upnp configure	Upnp configuration mode
154	net port-vlan	port vlan
155	net port-vlan lan_edit <portnamew>	Vlan port name range 1-4 .
156	net port-vlan wlan_edit <ssidName>	SSID to be edited.Use command 'show net wireless_vlan status 'to display all SSID's Name
157	net vlan-membership	vlan-membership

158	net vlan-membership lan_edit <portw>	net vlan membership for the vlan and Wlan port
159	net vlan-membership wlan_edit <ssidName>	SSID to be edited.Use command 'show net wireless_vlan status 'to display all SSID's Name
160	net multivlan	Multivlan server configure
161	net multivlan subnet	Multivlan Server configure
162	net multiVlan subnet edit <vlanID>	Multivlan server edit mode
163	net vlan	vlan Configuration Changes.
164	net vlan config	vlan configuration .
165	net vlan config add <vlan_id>	Add a vlan.
166	net vlan config edit <vlan_id>	Edit a configured vlan.
167	net vlan config delete <VlanId>	Delete a vlan.
168	net vlan config enable	Enable vlan configuration.
169	net vlan config disable	Disable vlan configuration.
170	net dmz	dmz configuration mode
171	net dmz configure	dmz configuration mode

The command security? at the CLI prompt would give the description of all the configuration commands in the branch security, which is as follows:

1	security advanced_network	Security advanced setup.
2	security advanced_network attack_checks	Firewall Security Checks setup.
3	security advanced_network attack_checks configure	Security Checks configuration mode.
4	security advanced_network ips	Security ips setup.
5	security advanced_network ips setup	Ips configuration mode.
6	security application_rules	Application Rules Configuration setup.
7	security application_rules add	application rules rules configuration mode.
8	security application_rules edit <row_id>	application rules rules configuration mode.
9	security application_rules delete <row_id>	application rules rules configuration mode.
10	security firewall custom_service	Custom Services Configuration setup.
11	security firewall custom_service add	custom services configuration mode.
12	security firewall custom_service edit <row_id>	custom services configuration mode.



13	security firewall custom_service delete <row_id>	custom services configuration mode.
14	security blocked_clients	Blocked Clients Configuration setup.
15	security blocked_clients add	Blocked Clients configuration mode.
16	security blocked_clients edit <row_id>	Blocked Clients configuration mode.
17	security blocked_clients delete <row_id>	Blocked Clients configuration mode.
18	security dynamic_filter	dynamic filtering configuration setup.
19	security dynamic_filter configure	security dynamic content filtering configuration.
20	security firewall	Firewall rules setup.
21	security firewall ipv4	Firewall IPv4 rules setup.
22	security firewall ipv4 configure	Firewall IPV4 rules configuration mode.
23	security firewall ipv4 default_outbound_policy <default_outbound_policy>	Firewall Settings, Default Outbound Policy configuration mode.
24	security firewall ipv4 edit <row_id>	Firewall IPV4 rules configuration mode.
25	security firewall ipv4 enable <row_id>	Firewall IPV4 rules configuration mode.
26	security firewall ipv4 disable <row_id>	Firewall IPV4 Rules configuration mode.
27	security firewall ipv4 delete <row_id>	Firewall IPV4 Rules configuration mode.
28	security firewall ipv4 move <row_id>	Firewall IPV4 Rule reordering mode.
29	security firewall algs	Firewall ALGs configuration mode.
30	security firewall ipv6	Firewall IPv6 rules setup.
31	security firewall ipv6 configure	Firewall IPV6 rules configuration mode.
32	security firewall ipv6 edit <row_id>	Firewall IPV6 rules configuration mode.
33	security firewall ipv6 enable <row_id>	Firewall IPV6 rules configuration mode.
34	security firewall ipv6 disable <row_id>	Firewall IPV6 Rules configuration mode.
35	security firewall ipv6 delete <row_id>	Firewall IPV6 Rules configuration mode.
36	security firewall ipv6 move <row_id>	Firewall IPV6 Rule reordering mode.
37	security firewall ipv6 default_outbound_policy <default_outbound_policy>	Firewall Settings, IPv6 Default Outbound Policy configuration mode.
38	security ids	IDS Configuration setup.

39	security ids configure	IDS configuration mode.
40	security session_settings	Session Settings Configuration setup.
41	security session_settings configure	Session Settings configuration mode.
42	security schedules	Schedules Configuration setup.
43	security schedules add	Schedules configuration mode.
44	security schedules edit <row_id>	Schedules configuration mode.
45	security schedules delete <row_id>	Schedules configuration mode.
46	security firewall smtpAlg	smtpAlg configuration setup.
47	security firewall smtpAlg approvedMailld	approvedMailld configuration setup.
48	security firewall smtpAlg blockedMailld	blockedMailld configuration setup.
49	security firewall smtpAlg subjectList	subjectList configuration setup.
50	security firewall smtpAlg configure	Smtplib configuration mode.
51	security firewall smtpAlg approvedMailld add	It allows Configure approved Mailld.
52	security firewall smtpAlg approvedMailld edit <row_id>	It allows to edit a approved Mailld.
53	security firewall smtpAlg approvedMailld delete <row_id>	It allows to delete a approved Mailld.
54	security firewall smtpAlg blockedMailld add	It allows to Configure a blocked Mailld.
55	security firewall smtpAlg blockedMailld edit <row_id>	It allows to edit a blocked Mailld.
56	security firewall smtpAlg blockedMailld delete <row_id>	It allows to delete a blocked Mailld.
57	security firewall smtpAlg subjectList add	It allows to add subject with Mailld and action.
58	security firewall smtpAlg subjectList edit <row_id>	It allows to edit subject with Mailld and action.
59	security firewall smtpAlg subjectList delete <row_id>	It allows to delete the configuration.
60	security mac_filter	source mac filter configuration mode.
61	security ip_or_mac_binding	ip mac binding configuration mode.
62	security mac_filter configure	source mac filter configuration mode.
63	security mac_filter source	.
64	security mac_filter source add	Source Mac Filter configuration mode.
65	security mac_filter source edit <row_id>	Source Mac Filter configuration mode.

66	security mac_filter source delete <row_id>	Source Mac Filter configuration mode.
67	security ip_or_mac_binding add	ip/mac binding configuration mode.
68	security ip_or_mac_binding edit <row_id>	ip/mac binding configuration mode.
69	security ip_or_mac_binding delete <row_id>	ip/mac binding configuration mode.
70	security firewall vpn_passthrough	VPN Passthrough setup.
71	security firewall vpn_passthrough configure	VPN Passthrough configuration mode.
72	security webAccess	Web Access Filter Configuration setup.
73	security webAccess status <status>	security webAccess status
74	security webAccess add	security webAccess add
75	security webAccess edit <row_id>	security webAccess edit
76	security webAccess delete <row_id>	security webAccess delete
77	security website_filter	website filtering configuration setup.
78	security website_filter content_filtering	content filtering configuration setup.
79	security website_filter approved_urls	trusted domains configuration setup.
80	security website_filter blocked_keywords	blocked keywords configuration setup.
81	security website_filter content_filtering configure	content filtering configuration mode.
82	security website_filter approved_urls add	trusted domains configuration mode.
83	security website_filter approved_urls edit <row_id>	trusted domains configuration mode.
84	security website_filter approved_urls delete <row_id>	trusted Domains configuration mode.
85	security website_filter blocked_keywords add	blocked Keyword configuration mode.
86	security website_filter blocked_keywords edit <row_id>	blocked Keywords configuration mode.
87	security website_filter blocked_keywords delete <row_id>	blocked Keywords configuration mode.

88	security website_filter blocked_keywords enable <row_id>	blocked Keywords configuration mode.
89	security website_filter blocked_keywords disable <row_id>	blocked Keywords configuration mode.

# Chapter 6. Configuration commands under branch VPN

## 6.1 vpn gre\_tunnel add

S.No	Command Name	Description	Type and Description
1	Save	Save system user configuration changes.	
2	Exit	Save system user configuration changes and exit current mode.	
3	Cancel	Roll back system user configuration changes.	
4	tunnelname	Enter the Tunnel Name here	String
5	ipaddress	Enter the tunnel IP Address here	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	subnet_mask	Enter the tunnel Subnet Mask here	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	Interface	Enter the Interface on which the tunnel is established on	WAN interface type
8	remote_ip	Enter the Remote IP to which the tunnel is being established here	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	ddp_broadcast	Select enable/disable DDP packet forwarding on the tunnel here	Boolean choice
10	route_network	Enter the destination network of GRE tunnel here	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	route_netmask	Enter the subnet mask of destination network here	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	gateway	Enter the gateway of the destination network here	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.2 vpn gre\_tunnel edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	GRE Tunnel configuration mode	Unsigned integer
2	save	Saves system user configuration changes.	
3	exit	Saves system user configuration changes and exit current mode.	
4	cancel	Roll back system user configuration changes.	
5	tunnelname	Enter the Tunnel Name here.	String
6	ipaddress	Enter the tunnel IP Address here.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	subnet_mask	Enter the tunnel Subnet Mask here.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	interface	Enter the Interface on which the tunnel is established on.	WAN interface type
9	remote_ip	Enter the Remote IP to which the tunnel is being established here.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	ddp_broadcast	Select enable/disable DDP packet forwarding on the tunnel here.	Boolean choice
11	route_network	Enter the destination network of GRE tunnel here.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	route_netmask	Enter the subnet mask of destination network here.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	gateway	Enter the gateway of the destination network here.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.3 vpn gre\_tunnel delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	GRE Tunnel delete mode	Unsigned integer

## 6.4 vpn l2tp client configure

S.No	Command Name	Description	Type and Description
1	save	Save l2tp client configuration changes.	
2	cancel	Roll back l2tp client configuration changes.	
3	exit	Save l2tp client configuration changes and exit current mode.	
4	enable	enable/disable L2TP client.	Boolean choice
5	server_address	L2TP server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	remote_network	Remote Network Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	remote_subnet	Remote Network Subnet Mask	number in range of 1 to 32
8	username	Username allocated to client	String
9	password	Password allocated to client	String
10	mppe_enable	Enable mppe encryption	Boolean choice
11	reconnect_mode	Select reconnect mode	Reconnect Mode type
12	time_out	Time Out	Radius client authentication timeout Type.
13	auto_dial	Auto Dial	Boolean choice
14	time	Client will try to connet to server after user specified time.	Client auto dial timeout Type.

## 6.5 vpn l2tp client\_action <action>

S.No	Command Name	Description	Type and Description
1	<action>	vpn l2tp client action set	Reconnect Mode type

## 6.6 vpn l2tp server configure

S.No	Command Name	Description	Type and Description
1	save	Save l2tp server configuration changes.	
2	cancel	Roll back l2tp server configuration changes.	

S.No	Command Name	Description	Type and Description
3	exit	Save l2tp server configuration changes and exit current mode.	
4	enable_v4	enable/disable L2TP server in IPv4 mode only.	Boolean choice
5	enable_v6	enable/disable L2TP server in IPv4/IPv6 mode.	Boolean choice
6	Routing_mode	select L2TP routing mode	Select Route Mode
7	start_address	L2TP server starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	end_address	L2TP server ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	ipv6_prefix	L2TP server IPv6 Prefix	String
10	ipv6_prefix_length	L2TP server IPv6 Prefix length	Unsigned integer
11	Authentication_type	Authentication type	Authentication type
12	EnablePap	enable pap authentication	Boolean choice
13	EnableChap	enable chap authentication	Boolean choice
14	EnableMSChap	enable MSChap authentication	Boolean choice
15	EnableMSChapv2	enable MSChapv2Enable authentication	Boolean choice
16	l2tpSecretKeyEnable	L2TP Enanle secret key	Boolean choice
17	secretKey	L2TP secret Key	String
18	timeout	User Time Out	Radius client authentication timeout Type.

## 6.7 vpn openvpn config

S.No	Command Name	Description	Type and Description
1	save	Save openvpn configuration changes	
2	cancel	Roll back openvpn configuration changes.	
3	exit	Save openvpn configuration changes and exit current mode.	
4	enable	enable/disable openvpn client/server	Boolean choice
5	mode	OpenVPN daemon mode. It can run in server mode, client	OpenVPN daemon mode.



S.No	Command Name	Description	Type and Description
		mode or access server client mode	
6	server_identifier_type	OpenVPN server identifier type	OpenVPN server identifier type
7	server_ip	OpenVPN server IP address/FQDN to which the client connect.	
8	server_ip ip_address	OpenVPN server IP address to which the client connect.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
9	server_ip fqdn	OpenVPN server FQDN to which the client connect.	String
10	vpn_network	Address of the Virtual Network	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
11	vpn_netmask	Netmask of the Virtual Network	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
12	port	The port number on which openvpn server(or Access Server) runs	Port number
13	tunnel_protocol	The protocol used to communicate with the remote host.Ex: Tcp, Udp. Udp is the default.	The protocol used to communicate with the remote host
14	encryption_algorithm	The cipher with which the packets are encrypted. Ex: BF-CBC, AES-128,AES-192 and AES-256. BF-CBC is the default	The cipher with which the packets are encrypted
15	hash_algorithm	Message digest algorithm used to authenticate packets. Ex: SHA1, SHA256 and SHA512. SHA1 is the default.	Message digest algorithm used to authenticate packets
16	tunnel_type	Select Full Tunnel to redirect all the traffic through the tunnel. Select Split Tunnel to redirect traffic to only specified resources (added from openVpnClient Routes) through the tunnel. Full Tunnel is the default.	type of tunnel
17	allow_client_to_client	Enable this to allow openvpn clients to communicate with	Boolean choice

S.No	Command Name	Description	Type and Description
		each other in split tunnel case. Disabled by default.	
18	select_primaryCert	Enable this to select Set of certificates and keys the server uses. Enable this for first time configuration	Boolean choice
19	select_secondaryCert	Enable this to select Set of certificates and keys newly uploaded.	Boolean choice
20	enable_tls_authkey	Enabling this adds Tls authentication which adds an additional layer of authentication. Can be checked only when the tls key is uploaded. Disabled by default.	Boolean choice
21	block_invalid_client_certificates	Enabling this blocks invalid client certificates based on the CRL certificate uploaded. Can be checked only when the CRL certificate is uploaded. Disabled by default.	Boolean choice
22	duplicate_cn	Enable this to allow multiple clients to connectd.	Boolean choice
23	user_based_auth	Enable this to allow clients to authenticate with server.	Boolean choice
24	username	username to authenticate to server.	String
25	password	password to authenticate to server.	String

## 6.8 vpn openvpn remote\_network add

S.No	Command Name	Description	Type and Description
1	save	Save Remote network changes	
2	cancel	Roll back Remote network configuration changes.	
3	exit	Save Remote network configuration changes and exit current mode.	
4	common_name	Common Name of the OpenVPN client certificate	String

S.No	Command Name	Description	Type and Description
5	remote_network	Network address of the remote resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	remote_netmask	Netmask of the remote resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.9 vpn openvpn remote\_network edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Remote network edit mode.	Unsigned integer
2	save	Saves Remote network changes.	
3	cancel	Roll back Remote network configuration changes.	
4	exit	Save Remote network configuration changes and exit current mode.	
5	common_name	Common Name of the OpenVPN client certificate.	String
6	remote_network	Network address of the remote resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	remote_netmask	Netmask of the remote resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.10 vpn openvpn remote\_network delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Openvpn remote network delete mode.	Unsigned integer

## 6.11 vpn openvpn local\_network add

S.No	Command Name	Description	Type and Description
1	save	Save local network changes.	
2	cancel	Roll back local network configuration changes	
3	exit	Save local network configuration changes and exit current mode.	

S.No	Command Name	Description	Type and Description
4	local_network	Network address of the local resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	local_netmask	Netmask of the local resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.12 vpn openvpn local\_network edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Local network edit mode.	Unsigned integer
2	save	Saves local network changes.	
3	cancel	Roll back local network configuration changes.	
4	exit	Save local network configuration changes, and exit current mode.	
5	local_network	Network address of the local resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	local_netmask	Netmask of the local resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.13 vpn openvpn local\_network delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	openvpn local network delete mode.	Unsigned integer

## 6.14 vpn openvpn cert\_upload ca <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	upload the pem formatted CA Certificate.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.15 vpn openvpn cert\_upload server\_client\_cert <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Upload the pem formatted Server / Client Certificate.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.16 vpn openvpn cert\_upload client\_key <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Upload the pem formatted Server/Client key.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.17 vpn openvpn cert\_upload dh\_Key <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Upload the pem formatted Diffie Hellman key.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.18 vpn openvpn cert\_upload tls\_Authkey <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Upload the pem formatted Tls Authentication Key	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.19 vpn openvpn cert\_upload crl\_cert <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Upload the pem formatted CRL Certificate.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.20 vpn openvpn cert\_upload config <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Upload the pem formatted config file.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.21 vpn pptp client configure

S.No	Command Name	Description	Type and Description
1	save	Save pptp client configuration changes.	
2	cancel	Roll back pptp client configuration changes.	
3	exit	Save pptp client configuration changes and exit current mode.	
4	enable	enable/disable PPTP client.	Boolean choice
5	server_address	PPTP server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	remote_network	Remote Network Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	remote_subnet	Remote Network Subnet Mask	number in range of 1 to 32
8	username	Username allocated to client	String
9	password	Password allocated to client	String
10	mppe_enable	Enable mppe encryption	Boolean choice
11	time_out	Time Out	Unsigned integer
12	auto_dial	Auto Dial	Boolean choice

S.No	Command Name	Description	Type and Description
13	time	Client will try to connect to server after user specified time.	Client auto dial timeout Type.

## 6.22 vpn ptp client\_action <action>

S.No	Command Name	Description	Type and Description
1	<action>	vpn ptp client action set.	Boolean choice

## 6.23 vpn ptp server configure

S.No	Command Name	Description	Type and Description
1	save	Save ptp server configuration changes.	
2	cancel	Roll back ptp server configuration changes.	
3	exit	Save ptp server configuration changes and exit current mode.	
4	enable_v4	enable/disable PPTP server in IPv4 mode only.	Boolean choice
5	enable_v6	enable/disable PPTP server in IPv4/IPv6 mode.	Boolean choice
6	Routing_Mode	Select Routing mode	Select Route Mode
7	start_address	PPTP server starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	end_address	PPTP server ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	ipv6_prefix	PPTP server IPv6 Prefix	String
10	ipv6_prefix_length	PPTP server IPv6 Prefix length	Unsigned integer
11	Authentication_type	Authentication type	Authentication type
12	pap_enable	PPTP server PAP authentication	Boolean choice
13	chap_enable	PPTP server CHAP authentication	Boolean choice
14	mschap_enable	PPTP server MSCHAP authentication	Boolean choice
15	mschapv2_enable	PPTP server MSCHAPV2 authentication	Boolean choice

S.No	Command Name	Description	Type and Description
16	Mppe40Enable	PPTP server Mppe40	Boolean choice
17	Mppe128Enable	PPTP server Mppe128	Boolean choice
18	MppeStatefulEnable	PPTP server MppeStateful	Boolean choice
19	UserTimeOut	PPTP server User TimeOut	Radius client authentication timeout Type.
20	Enable_Netbios	Enable the Netbios	Boolean choice
21	Primary_Wins_Server	Enter primary Wins server Ip Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
22	Secondary_Wins_Server	Secondary Wins server ip address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 6.24 vpn sslvpn portal-layouts add

S.No	Command Name	Description	Type and Description
1	save	Save portal settings	
2	exit	Save portal settings and exit current mode	
3	cancel	Roll back portal settings changes	
4	portal_name	Specify the portal name	String, Max of 31 alpha numeric characters
5	profile_name	Specify the profile name	String, Max of 32 alpha numeric characters
6	portal_title	Specify the portal title	String, Max 64 characters and no ' or empty space or "
7	banner_title	Specify the banner title	String, MAX 64 characters, ' is not supported;
8	banner_message	Specify the banner message	String, ' character is not supported;
9	display_banner	Specify whether the banner message should be displayed	Boolean choice
10	enable_httpmetatags	Specify whether the http meta tags should be enabled	Boolean choice
11	enable_activexwebcache cleaner	Specify whether the activex web cache cleaner should be enabled	Boolean choice
12	enable_vpntunnel	Specify whether the vpn tunnel should be enabled	Boolean choice
13	enable_portforwarding	Specify whether the port forwarding should be enabled	Boolean choice



S.No	Command Name	Description	Type and Description
14	sslAuthType	Authentication method for the portal.	Supported authentication type
15	SSL_GROUP	group name for the portal(only for local authentication).	String, Max 32 characters and no ' or empty space or "

## 6.25 vpn sslvpn portal-layouts edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Edit sslvpn portal layout	Unsigned integer
2	save	Save portal settings	
3	exit	Save portal settings and exit current mode	
4	cancel	Roll back portal settings changes	
5	profile_name	Specify the profile name	String, Max 32 characters and no ' or empty space or "
6	portal_title	Specify the portal title	String, Max 64 characters and no ' or empty space or "
7	banner_title	Specify the banner title	String, MAX 64 characters, ' is not supported;
8	banner_message	Specify the banner message	String, ' character is not supported;
9	display_banner	Specify whether the banner message should be displayed	Boolean choice
10	enable_httpmetatags	Specify whether the http meta tags should be enabled	Boolean choice
11	enable_activexwebcache cleaner	Specify whether the activex web cache cleaner should be enabled	Boolean choice
12	enable_vpntunnel	Specify whether the vpn tunnel should be enabled	Boolean choice
13	enable_portforwarding	Specify whether the port forwarding should be enabled	Boolean choice
14	SSL_GROUP	group name for the portal(only for local authentication).	String, Max 32 characters and no ' or empty space or "

## 6.26 vpn sslvpn portal-layouts delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete sslvpn portal layout.	Unsigned integer

## 6.27 vpn sslvpn portforwarding appconfig add

S.No	Command Name	Description	Type and Description
1	save	Save portforwarding Apps settings	
2	exit	Save portforwarding Apps settings and exit current mode	
3	cancel	Roll back portforwarding Apps settings changes	
4	serverip	Server ip address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	port	Server port	Port number

## 6.28 vpn sslvpn portforwarding appconfig delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete an application configuration rule	Unsigned integer

## 6.29 vpn sslvpn portforwarding hostconfig add

S.No	Command Name	Description	Type and Description
1	save	Saves portforwarding Host settings	
2	exit	Saves portforwarding Host settings and exit current mode	
3	cancel	Roll back portforwarding Host settings changes	
4	serverip	server ip address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	domain_name	domain name	String, Max 128 characters and no ' or empty space or "

## 6.30 vpn sslvpn portforwarding hostconfig delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete a host configuration rule.	Unsigned integer

## 6.31 vpn sslvpn resource add

S.No	Command Name	Description	Type and Description
1	save	Save sslvpn resource settings	
2	exit	Save sslvpn resource settings and exit current mode	
3	cancel	Roll back sslvpn resource settings changes	
4	resource_name	resource name	String, MAX 128 characters, ' is not supported;
5	service_type	service type	Sslvpn resource.

## 6.32 vpn sslvpn resource configure add <resource\_name>

S.No	Command Name	Description	Type and Description
1	<resource_name>	Add an sslvpn resource object.	String, MAX 128 characters, ' is not supported;
2	save	Save sslvpn resource object settings	
3	exit	Save sslvpn resource settings, and exit current mode.	
4	cancel	Roll back sslvpn resource settings changes	
5	object_type	object type	sslvpn resource object type.
6	object_address	object address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	mask_length	mask length	number in range of 1 to 32
8	start_port	start port	Port number
9	end_port	end port	Port number
10	icmp	include icmp	Source address type for users ip policy.

### 6.33 vpn sslvpn resource configure delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete an sslvpn resource object	Unsigned integer.

### 6.34 vpn sslvpn resource delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete an sslvpn resource	Unsigned integer

### 6.35 vpn sslvpn policy add

S.No	Command Name	Description	Type and Description
1	save	Save sslvpn policy settings	
2	exit	Save sslvpn policy settings and exit current mode	
3	cancel	Roll back sslvpn policy settings changes	
4	policy_type	policy type.	sslvpn policy type.
5	policy_owner	policy owner	String
6	destination_objecttype	destination object type	sslvpn policy destination type.
7	policy_name	policy name	String, character is not supported;
8	policy_address	policy address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	policy_masklength	policy masklength	number in range of 1 to 32
10	start_port	start port	Port number
11	end_port	end port	Port number
12	service_type	service type	sslvpn resource
13	resource_name	resource name	String, MAX 128 characters, ' is not supported;
14	policy_permission	policy permission	sslvpn policy type
15	icmp	include icmp traffic.	source address type for users ip policy

## 6.36 vpn sslvpn policy edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Edit an sslvpn policy	Unsigned integer
2	save	Save sslvpn policy settings	
3	exit	Save sslvpn policy settings, and exit current mode	
4	cancel	Roll back sslvpn policy settings changes	
5	policy_address	policy address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	policy_masklength	policy masklength	number in range of 1 to 32
7	start_port	start port.	Port number
8	end_port	end port.	Port number
9	resource_name	resource name	String, MAX 128 characters, ' is not supported.
10	policy_permission	policy permission	sslvpn policy type.
11	icmp	include icmp traffic.	source address type for users ip policy.

## 6.37 vpn sslvpn policy delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete an sslvpn policy	Unsigned integer.

## 6.38 vpn sslvpn client

S.No	Command Name	Description	Type and Description
1	save	Save sslvpn client settings	
2	exit	Save sslvpn client settings and exit current mode	
3	cancel	Roll back sslvpn client settings changes	
4	enable_fulltunnel	Enable split tunnel.	Boolean choice
5	dns_suffix	dns suffix	String
6	primary_dns	primary dns server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
7	secondary_dns	secondary dns server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
8	begin_clientaddress	Client Address Range Begin	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
9	end_clientaddress	Client Address Range End	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
10	lcp_timeout	lcp timeout	Unsigned integer

### 6.39 vpn sslvpn route add

S.No	Command Name	Description	Type and Description
1	save	Save sslvpn route settings	
2	exit	Save sslvpn route settings, and exit current mode.	
3	cancel	Roll back sslvpn route settings changes	
4	destination_network	destination network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
5	subnet_mask	subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

### 6.40 vpn sslvpn route delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete sslvpn client route	Unsigned integer

### 6.41 vpn ipsec policy configure <name>

S.No	Command Name	Description	Type and Description
1	<name>	vpn policy configuration mode	Only AtoZ, atoz and 0to9 characters are allowed
2	save	Save vpn policy configuration changes.	
3	cancel	Roll back vpn policy configuration changes.	
4	exit	Save vpn policy configuration changes and exit current mode.	
5	general_policy_type	Setting policy manual or auto	vpn policy type

S.No	Command Name	Description	Type and Description
6	general_ike_version	Setting version ikev1 or ikev2	IPsec VPN IKE Version
7	general_ip_protocol_version	Setting protocol version ipv4 or ipv6	vpn protocol version
8	general_select_local_gateway	Setting local gateway for the vpn policy	VPN gateway
9	general_remote_end_point_type	Set mode to IP address or Internet Name/FQDN of the remote gateway or client PC	vpn remote end point type
10	general_remote_end_point	The IP address or Internet Name/FQDN of the remote gateway or client PC.	
11	general_remote_end_point_ip_address	The IP address of the remote gateway or client PC.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
12	general_remote_end_point_fqdn	The IP address or Internet Name/FQDN of the remote gateway or client PC.	String
13	general_enable_mode_config	enable/disable mode config	Boolean choice
14	general_enable_netbios	enable/disable this to allow NetBIOS broadcasts to travel over the VPN tunnel.	Boolean choice
15	general_enable_rollover	enable/disable rollover	Boolean choice
16	general_protocol	Setting protocol esp or ah	IPsec VPN Protocol
17	general_enable_dhcp	enable/disable dhcp.	Boolean choice
18	general_redundant_vpn_gateway	enable/disable Redundant vpn gateway	Boolean choice
19	general_backup_policy_name	backup policy name	String
20	general_failback_time	Failback time to switch from back-up to primary	Unsigned integer
21	general_local_network_type	Select the IP addresses on the local side that will be part of the tunnel. This can be either a single IP address, several IP addresses in a range, an entire subnet, or any IP address that wants to connect	vpn network type
22	general_local_start_address	IP address from where the range needs to begin	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6

S.No	Command Name	Description	Type and Description
23	general_local_end_address	IP address where the range needs to end	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
24	general_local_subnet_mask	Subnet mask of the subnet used	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
25	general_local_prefix_length	Prefix length of the ipv6 subnet used	IPv6 Prefix length
26	general_remote_network_type	Select the IP addresses on the remote side that will be part of the tunnel. This can be either a single IP address, several IP addresses in a range, an entire subnet, or any IP address that wants to connect	vpn network type
27	general_remote_start_address	IP address from where the range needs to begin	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
28	general_remote_end_address	IP address where the range needs to end	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
29	general_remote_subnet_mask	Subnet mask of the subnet used	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
30	general_remote_prefix_length	Prefix length of the ipv6 subnet used	IPv6 Prefix length
31	general_enable_keepalive	enable/disable keepalive	Boolean choice
32	general_keepalive_sourceip	keepalive sourceip	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
33	general_keepalive_destinationip	keepalive destinationip	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
34	general_keepalive_detection_period	keepalive detection period	keepalive detection period in seconds
35	general_keepalive_failure_count	keepalive failure count	keepalive failure count
36	general_l2tp_mode	Setting l2tp mode as None(0) or Client(1) or Gateway(2)	IPsec L2tp Mode
37	manual_spi_in	Takes a hexadecimal value between 3 and 8 characters.	Takes a hexadecimal value between 3 and 8 characters
38	manual_spi_out	Takes a hexadecimal value between 3 and 8 characters.	Takes a hexadecimal value between 3 and 8 characters



S.No	Command Name	Description	Type and Description
39	manual_encryption_algorithm	The algorithm used to encrypt the data	vpn encryption algorithm
40	manual_key_length	The key length for the algorithm.	Unsigned integer
41	manual_encryption_key_in	Encryption key of the inbound policy. The length of the key depends on the algorithm chosen	String
42	manual_encryption_key_out	Encryption key of the outbound policy. The length of the key depends on the algorithm chosen.	String
43	manual_authentication_algorithm	Algorithm used to verify the integrity of the data.	vpn authentication algorithm
44	manual_authentication_key_in	This is the integrity key (for ESP with Integrity-mode) for the inbound policy and depends on the algorithm chosen	String
45	manual_authentication_key_out	This is the integrity key (for ESP with Integrity-mode) for the outbound policy and depends on the algorithm chosen	String
46	auto_phase1_exchange_mode	Setting IKE exchange Mode	VPN Exchange Mode
47	auto_phase1_enable_nat_traversal	Enabling/Disabling Nat traversal	Boolean choice
48	auto_phase1_nat_keepalive_frequency	Setting IKE nat alive frequency	Unsigned integer
49	auto_phase1_local_identifier_type	Setting IKE local identifier type	IPsec VPN IKE local identifier type
50	auto_phase1_direction_type	Setting IKE direction type	IPsec VPN IKE direction Mode
51	auto_phase1_local_identifier	Setting IKE local identifier	String
52	auto_phase1_remote_identifier_type	Setting IKE remote identifier	IPsec VPN IKE local identifier type
53	auto_phase1_remote_identifier	Setting IKE remote identifier	String
54	auto_phase1_encryption_algorithm	Setting IKE encryption algorithm	
55	auto_phase1_encryption_algorithm DES	Setting IKE encryption algorithm	

S.No	Command Name	Description	Type and Description
56	auto_phase1_encrypti on_algorithm DES enable_DES	Enable DES encryption algorithm	Boolean choice
57	auto_phase1_encrypti on_algorithm 3DES	Setting IKE encryption algorithm	
58	auto_phase1_encrypti on_algorithm 3DES enable_3DES <3des>	Enable 3DES encryption algorithm	Boolean choice
59	auto_phase1_encrypti on_algorithm AES- 128	Setting IKE encryption algorithm	
60	auto_phase1_encrypti on_algorithm AES- 128 enable_AES-128	Enable AES-128 encryption algorithm	Boolean choice
61	auto_phase1_encrypti on_algorithm AES- 192	Setting IKE encryption algorithm	
62	auto_phase1_encrypti on_algorithm AES- 192 enable_AES-192	Enable AES-192 encryption algorithm	Boolean choice
63	auto_phase1_encrypti on_algorithm AES- 256	Setting IKE encryption algorithm	
64	auto_phase1_encrypti on_algorithm AES- 256 enable_AES-256	Enable AES-256 encryption algorithm	Boolean choice
65	auto_phase1_encrypti on_algorithm BLOWFISH	Setting IKE encryption algorithm	
66	auto_phase1_encrypti on_algorithm BLOWFISH enable_BLOWFISH	Enable BLOWFISH encryption algorithm	Boolean choice
67	auto_phase1_encrypti on_algorithm BLOWFISH keylength	Enter BLOWFISH keylength	Unsigned integer
68	auto_phase1_encrypti on_algorithm CAST128	Setting IKE encryption algorithm	
69	auto_phase1_encrypti on_algorithm CAST128 enable_CAST128	Enable CAST128 encryption algorithm	Boolean choice
70	auto_phase1_encrypti on_algorithm CAST128 keylength	Enter CAST128 keylength	Unsigned integer

S.No	Command Name	Description	Type and Description
71	auto_phase1_auth_algorithm	Setting IKE authentication algorithm	
72	auto_phase1_auth_algorithm MD5	Setting IKE authentication algorithm	
73	auto_phase1_auth_algorithm MD5 enable_MD5	Enable MD5 authentication algorithm	Boolean choice
74	auto_phase1_auth_algorithm SHA1	Setting IKE authentication algorithm	
75	auto_phase1_auth_algorithm SHA1 enable_SHA1	Enable SHA1 authentication algorithm	Boolean choice
76	auto_phase1_auth_algorithm SHA2-256	Setting IKE authentication algorithm	
77	auto_phase1_auth_algorithm SHA2-256 enable_SHA2-256	Enable SHA2-256 authentication algorithm	Boolean choice
78	auto_phase1_auth_algorithm SHA2-384	Setting IKE authentication algorithm	
79	auto_phase1_auth_algorithm SHA2-384 enable_SHA2-384	Enable SHA2-384 authentication algorithm	Boolean choice
80	auto_phase1_auth_algorithm SHA2-512	Setting IKE authentication algorithm	
81	auto_phase1_auth_algorithm SHA2-512 enable_SHA2-512	Enable SHA2-512 authentication algorithm	Boolean choice
82	auto_phase1_auth_method	Setting IKE authentication algorithm method	IPsec VPN IKE authentication algorithm method
83	auto_phase1_dh_group	Setting IKE Diffie-Hellman (DH) Group	IPsec VPN IKE Diffie-Hellman (DH) Group type
84	auto_phase1_sa_lifetime	Setting IKE SA lifetime in seconds	Unsigned integer
85	auto_phase1_pre_shared_key	Setting IKE pre shared key	Only AtoZ, atoz and 0to9 characters are allowed
86	auto_phase1_enable_dead_peer_detection	Enabling/Disabling dead peer detection	Boolean choice
87	auto_phase1_detection_period	Setting dead peer detection time period	Unsigned integer
88	auto_phase1_reconnect_failure_count	Setting dead peer detection failure count	Unsigned integer
89	auto_phase1_extended_authentication	setting extended authentication method	IPsec VPN IKE extended authentication method
90	auto_phase1_authentication_type	setting extended authentication type	IPsec VPN IKE extended authentication method

S.No	Command Name	Description	Type and Description
91	auto_phase1_xauth_username	Username for extended authentication	String
92	auto_phase1_xauth_password	Password for extended authentication	String
93	auto_phase2_sa_lifetime	vpn auto policy phase2 configure	
94	auto_phase2_sa_lifetime seconds	Setting IKE SA lifetime in seconds	Unsigned integer
95	auto_phase2_sa_lifetime bytes	Setting IKE SA lifetime in bytes	Unsigned integer
96	auto_phase2_encryption_algorithm	Setting IKE encryption algorithm	
97	auto_phase2_encryption_algorithm DES	Setting IKE encryption algorithm	
98	auto_phase2_encryption_algorithm DES enable_DES	Enable DES encryption algorithm	Boolean choice
99	auto_phase2_encryption_algorithm 3DES	Setting IKE encryption algorithm	
100	auto_phase2_encryption_algorithm 3DES enable_3DES <3des>	Enable 3DES encryption algorithm	Boolean choice
101	auto_phase2_encryption_algorithm AES-128	Setting IKE encryption algorithm	
102	auto_phase2_encryption_algorithm AES-128 enable_AES-128	Enable AES-128 encryption algorithm	Boolean choice
103	auto_phase2_encryption_algorithm AES-192	Setting IKE encryption algorithm	
104	auto_phase2_encryption_algorithm AES-192 enable_AES-192	Enable AES-192 encryption algorithm	Boolean choice
105	auto_phase2_encryption_algorithm AES-256	Setting IKE encryption algorithm	
106	auto_phase2_encryption_algorithm AES-256 enable_AES-256	Enable AES-256 encryption algorithm	Boolean choice
107	auto_phase2_encryption_algorithm TWOFISH-128	Setting IKE encryption algorithm	
108	auto_phase2_encryption_algorithm TWOFISH-128 enable_TWOFISH-128	Enable TWOFISH-128 encryption algorithm	Boolean choice

S.No	Command Name	Description	Type and Description
	TWOFISH-128 enable_TWOFISH-128		
109	auto_phase2_encrypti on_algorithm TWOFISH-192	Setting IKE encryption algorithm	
110	auto_phase2_encrypti on_algorithm TWOFISH-192 enable_TWOFISH-192	Enable TWOFISH-192 encryption algorithm	Boolean choice
111	auto_phase2_encrypti on_algorithm TWOFISH-256	Setting IKE encryption algorithm	
112	auto_phase2_encrypti on_algorithm TWOFISH-256 enable_TWOFISH-256	Enable TWOFISH-256 encryption algorithm	Boolean choice
113	auto_phase2_encrypti on_algorithm BLOWFISH	Setting IKE encryption algorithm	
114	auto_phase2_encrypti on_algorithm BLOWFISH enable_BLOWFISH	Enable BLOWFISH encryption algorithm	Boolean choice
115	auto_phase2_encrypti on_algorithm BLOWFISH keylength	Enter BLOWFISH keylength	Unsigned integer
116	auto_phase2_encrypti on_algorithm CAST128	Setting IKE encryption algorithm	
117	auto_phase2_encrypti on_algorithm CAST128 enable_CAST128	Enable CAST128 encryption algorithm	Boolean choice
118	auto_phase2_encrypti on_algorithm CAST128 keylength	Enter CAST128 keylength	Unsigned integer
119	auto_phase2_auth_al gorithm	Setting IKE authentication algorithm	
120	auto_phase2_auth_al gorithm MD5	Setting IKE authentication algorithm	
121	auto_phase2_auth_al gorithm MD5 enable_MD5	Enable MD5 authentication algorithm	Boolean choice

S.No	Command Name	Description	Type and Description
122	auto_phase2_auth_algorithm SHA1	Setting IKE authentication algorithm	
123	auto_phase2_auth_algorithm SHA1 enable_SHA1	Enable SHA1 authentication algorithm	Boolean choice
124	auto_phase2_auth_algorithm SHA2-256	Setting IKE authentication algorithm	
125	auto_phase2_auth_algorithm SHA2-256 enable_SHA2-256	Enable SHA2-256 authentication algorithm	Boolean choice
126	auto_phase2_auth_algorithm SHA2-384	Setting IKE authentication algorithm	
127	auto_phase2_auth_algorithm SHA2-384 enable_SHA2-384	Enable SHA2-384 authentication algorithm	Boolean choice
128	auto_phase2_auth_algorithm SHA2-224	Setting IKE authentication algorithm	
129	auto_phase2_auth_algorithm SHA2-224 enable_SHA2-224	Enable SHA2-224 authentication algorithm	Boolean choice
130	auto_phase2_auth_algorithm SHA2-512	Setting IKE authentication algorithm	
131	auto_phase2_auth_algorithm SHA2-512 enable_SHA2-512	Enable SHA2-512 authentication algorithm	Boolean choice
132	auto_phase2_enable_pfskeygroup	Enable/Disable PFS key group	Boolean choice
133	auto_phase2_dh_group	Setting IKE Diffie-Hellman (DH) Group	IPsec VPN IKE Diffie-Hellman (DH) Group type

## 6.42 vpn ipsec dhcp configure

S.No	Command Name	Description	Type and Description
1	save	Save vpn ipsec dhcp configuration changes.	
2	cancel	Roll back vpn ipsec dhcp configuration changes.	
3	exit	Save vpn ipsec dhcp configuration changes and exit current mode.	
4	start_address	Setting ipsec dhcp start address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
5	end_address	Setting ipsec dhcp end address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	subnet_mask	Setting ipsec dhcp subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

### 6.43 vpn ipsec policy enable <name>

S.No	Command Name	Description	Type and Description
1	<name>	Enable a vpn policy	Only AtoZ, atoz and 0to9 characters are allowed

### 6.44 vpn ipsec policy disable <name>

S.No	Command Name	Description	Type and Description
1	<name>	Disable a vpn policy	Only AtoZ, atoz and 0to9 characters are allowed

### 6.45 vpn ipsec policy delete <name>

S.No	Command Name	Description	Type and Description
1	<name>	Delete a vpn policy	Only AtoZ, atoz and 0to9 characters are allowed

### 6.46 vpn ipsec policy connect <name>

S.No	Command Name	Description	Type and Description
1	<name>	Connect a vpn tunnel	Only AtoZ, atoz and 0to9 characters are allowed

### 6.47 vpn ipsec policy drop <name>

S.No	Command Name	Description	Type and Description
1	<name>	Drop a vpn tunnel	Only AtoZ, atoz and 0to9 characters are allowed

## Chapter 7. Configuration commands under branch DOT11

### 7.1 dot11 profile add <profile\_name>

S.No	Command Name	Description	Type and Description
1	<profile_name>	802.11 profile configuration mode.	Only AtoZ, atoz and 0to9 characters are allowed
2	Save	Save profile configuration changes	
3	Exit	Save profile configuration changes and exit current mode.	
4	Ssid	Set the 802.11 profile SSID.	String
5	broadcast-ssid	Enable or disable SSID broadcast.	Boolean choice
6	security_type	Set the profile security type.	802.11 Security Types
7	Wep	Set profile WEP options.	
8	wep authentication	Set WEP authentication type.	WEP Authentication Types
9	wep encryption	Set WEP encryption type.	WEP Encryption Types
10	wep key	Set WEP key. Not required if passphrase is set.	WEP key index type (1-4) String
11	wep passphrase	Set WEP passphrase to generate WEP key from.	WEP key index type (1-4) String
12	Wpa	Set the WPA options.	
13	wpa authentication	Set WPA authentication type.	WPA Authentication Types
14	wpa encryption	Set WPA encryption type.	WPA Encryption Types
15	wpa wpa- password	WPA Password. Needed only if authentication is PSK	String

### 7.2 dot11 profile edit <profile\_name>

S.No	Command Name	Description	Type and Description
1	<profile_name>	802.11 profile configuration mode.	Only AtoZ, atoz and 0to9 characters are allowed
2	Save	Save profile configuration changes	
3	Exit	Save profile configuration changes and exit current mode.	
4	Ssid	Set the 802.11 profile SSID.	String



S.No	Command Name	Description	Type and Description
5	broadcast-ssid	Enable or disable SSID broadcast.	Boolean choice
6	security_type	Set the profile security type.	802.11 Security Types
7	Wep	Set profile WEP options.	
8	wep authentication	Set WEP authentication type.	WEP Authentication Types
9	wep encryption	Set WEP encryption type.	WEP Encryption Types
10	wep key	Set WEP key. Not required if passphrase is set.	WEP key index type (1-4) String
11	wep passphrase	Set WEP passphrase to generate WEP key from.	WEP key index type (1-4) String
12	wpa	Set the WPA options.	
13	wpa authentication	Set WPA authentication type.	WPA Authentication Types
14	wpa encryption	Set WPA encryption type.	WPA Encryption Types
15	wpa wpa- password	WPA Password. Needed only if authentication is PSK	String

## 7.3 dot11 radius configure

S.No	Command Name	Description	Type and Description
1	save	Save radius configuration changes.	
2	cancel	Roll back radius configuration changes	
3	exit	Save ACL configuration changes and exit current mode.	
4	primary_server	Set Radius Primary authentication Server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	secondary_server	Set Radius Seconadry authentication Server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	port	Set port number.	number in range of 0 to 65535
7	secret	Set secret key for radius.	String
8	timeout	Set timeout for radius client.	Radius client authentication timeout Type.
9	retries	Authentication retries limit to radius server.	Radius client authentication timeout Type.

## 7.4 dot11 profile delete <profile\_name>

S.No	Command Name	Description	Type and Description
1	<profile_name>	Delete an 802.11 profile.	Only A to Z, a to z and 0 to 9 characters are allowed

## 7.5 dot11 accesspoint configure <ap\_name>

S.No	Command Name	Description	Type and Description
1	<ap_name>	802.11 access point configuration mode	Only AtoZ, atoz and 0to9 characters are allowed
2	save	Save AP configuration changes	
3	cancel	Roll back AP configuration changes	
4	exit	Save AP configuration changes and exit current mode.	
5	profile	Set the 802.11 profile the AP will use.	String
6	wlan_partition	Enable or Disable wlan_partition.	Boolean choice
7	scheduleControl	Enable or Disable schedule control.	Boolean choice
8	enable_active_time	Setting time.	Boolean choice
9	start	Setting the time limits.	
10	stop	Setting the time limits.	
11	start hour	Setting the time limits.	H(1-12) using 12 hour clock
12	stop hour	Setting the time limits.	H(1-12) using 12 hour clock
13	start minute	Setting the time limits.	minute in the format MM(00-59)
14	stop minute	Setting the time limits.	minute in the format MM(00-59)
15	start meridian	Setting the time limits.	Schedule Meridiem Types.
16	stop meridian	Setting the time limits.	Schedule Meridiem Types.

## 7.6 dot11 accesspoint delete <ap\_name>

S.No	Command Name	Description	Type and Description
1	<ap_name>	Delete an 802.11 access point.	Only AtoZ, atoz and 0to9 characters are allowed

## 7.7 dot11 accesspoint disable <ap\_name>

S.No	Command Name	Description	Type and Description
1	<ap_name>	Disable an 802.11 access point	Only AtoZ, atoz and 0to9 characters are allowed

## 7.8 dot11 accesspoint enable <ap\_name>

S.No	Command Name	Description	Type and Description
1	<ap_name>	Enable an 802.11 access point	Only AtoZ, atoz and 0to9 characters are allowed

## 7.9 dot11 radio configure

S.No	Command Name	Description	Type and Description
1	save	Save radio configuration changes.	
2	cancel	Roll back radio configuration changes	
3	exit	Save radio configuration changes and exit current mode.	
4	channel	Set the channel used by radio.	Dot11 Radio Channels.
5	default-transmit-power	Set default trans power for APs using this radio.	Dot11 Radio default transmit power.
6	operating_frequency	Set dot11 radio operating frequency.	Dot11 Radio operating frequency band
7	2.4mode	Set dot11 radio mode.	Dot11 Radio Mode
8	transmission_rate	Set Transmission Rate for the radio.	Dot11 Radio Transmission Rate
9	channel_spacing	Set channel spacing for the radio.	Radio Channel Spacing.
10	control_side_band	Set control band for radio.	Dot11 Radio control band

## 7.10 dot11 radio advanced configure

S.No	Command Name	Description	Type and Description
1	save	Save advanced AP configuration changes	
2	cancel	Roll back advanced AP configuration changes	

S.No	Command Name	Description	Type and Description
3	exit	Save advanced AP configuration changes and exit current mode.	
4	beacon_interval	Set the time between beacon transmissions (in milliseconds).	Dot11 BEACON Interval.
5	dtim_interval	Set the interval between delivery traffic indication message.	Dot11 Dtim Interval.
6	rts_threshold	Set the Request to Send (RTS) threshold.	Dot11 Rts threshold Interval.
7	fragmentation_threshold	Set the maximum length of the frame.	Dot11 Fragmentation Interval.
8	preamble_mode	Set the 802.11b preamble type to be prepended to every frame	802.11b Preamble Types
9	protection_mode	Enable/disable RTS/CTS handshake before packet transmission.	RTSCTS Protection mode
10	short_retry_limit	Set the retry limit for frame retransmission on transmission failure.	802.11 Retry Limit
11	long_retry_limit	Set the retry limit for frame retransmission on transmission failure.	802.11 Retry Limit
12	power_save_enable	Enable/Disable power save mode.	Boolean choice

## 7.11 dot11 radio advanced MulToUni configure

S.No	Command Name	Description	Type and Description
1	save	Save advanced AP MulToUni configuration changes	
2	cancel	Roll back advanced AP MulToUni configuration changes	
3	exit	Save advanced AP MulToUni configuration changes and exit current mode.	
4	Multi_To_Unicast	Enable/Disable Multi To Unicast mode.	Boolean choice

## 7.12 dot11 accesspoint wps configure

S.No	Command Name	Description	Type and Description
1	save	Save WPS configuration changes	
2	cancel	Roll back WPS configuration changes	
3	exit	Save WPS configuration changes and exit current mode.	
4	access_point	Access point.	String
5	wps_status	WPS status.	WPS status
6	configure_via_pin	configure WPS via PIN.	Boolean choice
7	configure_via_pbc	configure WPS via PBC.	Boolean choice
8	station_pin	Set PIN for WPS config.	String

## 7.13 dot11 accesspoint ACL configure <ap\_name>

S.No	Command Name	Description	Type and Description
1	<ap_name>	802.11 AP ACL configuration mode.	Only AtoZ, atoz and 0to9 characters are allowed
2	save	Save AP ACL configuration changes.	
3	cancel	Roll back AP ACL configuration changes	
4	exit	Save AP ACL configuration changes and exit current mode.	
5	acl_policy	Set accesspoint ACL Policy.	Accesspoint ACL Policy type
6	mac_address	Set accesspoint ACL Policy.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

## 7.14 dot11 wds configure

S.No	Command Name	Description	Type and Description
1	save	Save WDS configuration changes	
2	cancel	Roll back WDS configuration changes	
3	exit	Save WDS configuration changes and exit current mode.	
4	wds_enable	Enable or Disable WDS.	Boolean choice

S.No	Command Name	Description	Type and Description
5	wds_passphrase	Enter WDS passphrase.	String, MIN 8 and MAX 63 characters are supported

### 7.15 dot11 wds mac\_address add *<mac\_address>*

S.No	Command Name	Description	Type and Description
1	<i>&lt;mac_address&gt;</i>	add wds peer mac address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

### 7.16 dot11 wds mac\_address delete *<rowid>*

S.No	Command Name	Description	Type and Description
1	<i>&lt;rowid&gt;</i>	deletes the wds peer mac_address.	Unsigned integer

# Chapter 8. Configuration commands under branch SYSTEM

## 8.1 System NT-Domain-Settings

S.No	Command Name	Description	Type and Description
1	save	Save NT Domain configuration changes.	
2	exit	Save NT Domain configuration changes and exit.	
3	cancel	Roll back configuration changes	
4	Authentication_Server_1	Set primary server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	Authentication_Server_2	Set Second alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	Authentication_Server_3	Set third alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	workgroup	Set NT Domain Workgroup	String
8	second_workgroup	Set second alternative Workgroup	String
9	third_workgroup	Set Third alternative Workgroup	String
10	timeout	Set NT Domain server connection timeout.	Unsigned integer
11	retries	Set NT Domain server connection retry attempts.	Unsigned integer
12	first_admin_name	Set NT Domain first server admin name	String
13	first_admin_passwd	Set NT Domain first server admin password	String
14	first_admin_hostname	Set NT Domain first server admin hostname	String
15	second_admin_name	Set NT Domain second server admin name	String
16	second_admin_passwd	Set NT Domain second server admin password	String
17	second_admin_hostname	Set NT Domain second server admin hostname	String

S.No	Command Name	Description	Type and Description
18	third_admin_name	Set NT Domain third server admin name	String
19	third_admin_passwd	Set NT Domain third server admin password	String
20	third_admin_hostname	Set NT Domain third server admin hostname	String
21	serverCheck	Check the reachability of configured servers.	

## 8.2 system Active-Directory-Settings

S.No	Command Name	Description	Type and Description
1	save	Save Active Directory Configuration changes.	
2	exit	Save Active Directory configuration changes and exit.	
3	cancel	Roll back configuration changes	
4	Authentication_Server_1	Set primary server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	Authentication_Server_2	Set second alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	Authentication_Server_3	Set third alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	Active_Directory_Domain	Set Active Directory Domain	String
8	Second_Active_Directory_Domain	Set Second Alternative Active Directory Domain	String
9	Third_Active_Directory_Domain	Set Third Alternative Active Directory Domain	String
10	timeout	Set Active Directory domain connection timeout.	Unsigned integer
11	retries	Set Active Directory connection retry attempts.	Unsigned integer
12	first_admin_name	Set Active Directory first server admin name	String
13	first_admin_passwd	Set Active Directory first server admin password	String
14	first_admin_hostname	Set Active Directory first	



S.No	Command Name	Description	Type and Description
		server admin hostname	String
15	second_admin_name	Set Active Directory second server admin name	String
16	second_admin_password	Set Active Directory second server admin password	String
17	second_admin_hostname	Set Active Directory second server admin hostname	String
18	third_admin_name	Set Active Directory third server admin name	String
19	third_admin_password	Set Active Directory third server admin password	String
20	third_admin_hostname	Set Active Directory third server admin hostname	String
21	serverCheck	Check the reachability of configured servers.	

### 8.3 system LDAP\_Settings

S.No	Command Name	Description	Type and Description
1	save	Save LDAP configuration changes.	
2	exit	Save LDAP configuration changes and exit.	
3	cancel	Roll back configuration changes	
4	Authentication_Server_1	Set primary server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	Authentication_Server_2	Set second alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	Authentication_Server_3	Set third alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	LDAP_Base_DN	Set LDAP Base DN	String
8	Second_LDAP_Base_DN	Set second alternative LDAP Base DN	String
9	Third_LDAP_Base_DN	Set Third alternative LDAP Base DN	String
10	LDAPAttribute1	Set LDAP Attribute 1	String
11	LDAPAttribute2	Set LDAP Attribute 2	String
12	LDAPAttribute3	Set LDAP Attribute 3	String
13	LDAPAttribute4	Set LDAP Attribute 4	String

S.No	Command Name	Description	Type and Description
14	timeout	Set LDAP server connection timeout.	Unsigned integer
15	retries	Set LDAP server connection retry attempts.	Unsigned integer
16	first_admin_name	Set LDAP first server admin name	String
17	first_admin_passwd	Set LDAP first server admin password	String
18	second_admin_name	Set LDAP second server admin name	String
19	second_admin_passwd	Set LDAP second server admin password	String
20	third_admin_name	Set LDAP third server admin name	String
21	third_admin_passwd	Set LDAP third server admin password	String
22	serverCheck	Check the reachability of configured servers.	

## 8.4 system POP3\_Settings POP3\_Server\_Configuration

S.No	Command Name	Description	Type and Description
1	save	Save POP3 configuration changes.	
2	exit	Save POP3 configuration changes and exit.	
3	cancel	Roll back configuration changes	
4	Authentication_Server_1	Set primary server.	String
5	Authentication_Server_2	Set secondary server.	String
6	Authentication_Server_3	Set optional server.	String
7	Authentication_Port_1	Set port for primary server	Port number
8	Authentication_Port_2	Set port for secondary server	Port number
9	Authentication_Port_3	Set port for optional server	Port number
10	SSL_Enable_1	Enable SSL for primary server.	Boolean choice
11	SSL_Enable_2	Enable SSL for secondary server.	Boolean choice

S.No	Command Name	Description	Type and Description
12	SSL_Enable_3	Enable SSL for optional server.	Boolean choice
13	CA_File_1	CAFILE for primary server.	String
14	CA_File_2	CAFILE for secondary server.	String
15	CA_File_3	CAFILE for optional server.	String
16	serverCheck	Check the reachability of configured servers.	

## 8.5 system POP3\_Settings POP3\_Trusted\_CA

S.No	Command Name	Description	Type and Description
1	exit	Exits POP3_Trusted_CA.	
2	add	Adds a certificate.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
3	delete	Delete a certificate.	String

## 8.6 system logging ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save logging configuration changes.	
2	exit	Save logging configuration changes and exit current mode.	
3	cancel	Roll back logging configuration changes.	
4	lan_wan_accept_packet_logs	lan to wan accepted Pkts Enable/Disable	Boolean choice
5	lan_wan_drop_packet_logs	lan to wan dropped Pkts Enable/Disable	Boolean choice
6	wan_lan_accept_packet_logs	wan to lan accepted Pkts logs Enable/Disable	Boolean choice
7	wan_lan_drop_packet_logs	wan to lan dropped Pkts logs Enable/Disable	Boolean choice
8	wan_dmz_accept_packet_logs	wan to dmz accepted Pkts logs Enable/Disable	Boolean choice
9	wan_dmz_drop_packet_logs	wan to dmz dropped Pkts logs Enable/Disable	Boolean choice
10	dmz_wan_accept_packet_logs	dmz to wan accepted Pkts logs Enable/Disable	Boolean choice

S.No	Command Name	Description	Type and Description
11	dmz_wan_drop_packet_logs	dmz to wan dropped Pkts logs Enable/Disable	Boolean choice
12	dmz_lan_accept_packet_logs	dmz to lan accepted Pkts logs Enable/Disable	Boolean choice
13	dmz_lan_drop_packet_logs	dmz to lan dropped Pkts logs Enable/Disable	Boolean choice
14	lan_dmz_accept_packet_logs	lan to dmz accepted Pkts logs Enable/Disable	Boolean choice
15	lan_dmz_drop_packet_logs	lan to dmz dropped Pkts logs Enable/Disable	Boolean choice
16	unicast_traffic_logs	All Unicast Traffic logs Enable/Disable	Boolean choice
17	broadcast_or_multicast_traffic_logs	All Broadcast/Multicast Traffic logs Enable/Disable	Boolean choice
18	bandwidth_limit_logs	Bandwidth Limit logs Enable/Disable	Boolean choice
19	ftp_logs	FTP logs Enable/Disable	Boolean choice
20	icmp_redirect_logs	Redirected ICMP Packets logs Enable/Disable	Boolean choice
21	log_invalid_packet	Log invalid packet Enable/Disable	Boolean choice
22	vlan_vlan_accept_packet_logs	vlan to vlan accepted Pkts Enable/Disable	Boolean choice
23	vlan_vlan_drop_packet_logs	vlan to vlan dropped Pkts Enable/Disable	Boolean choice
24	wcf_accept_packet_logs	WCF accepted Pkts Enable/Disable	Boolean choice
25	wcf_drop_packet_logs	WCF dropped Pkts Enable/Disable	Boolean choice
26	remote_classification_server_logs	Remote classification Server Logs Enable/Disable	Boolean choice

## 8.7 system logging facility configure <facility>

S.No	Command Name	Description	Type and Description
1	<facility>	System logging facility configuration mode.	String
2	save	Save log Facility configuration changes.	
3	exit	Save log facility configuration changes and exit current mode.	

S.No	Command Name	Description	Type and Description
4	cancel	Roll back log Facility configuration changes.	
5	level_options_set	Set level options. This command can be run multiple times in this view to set different level options.	Logging Facility Type. Logging Level Options Type. Boolean choice

## 8.8 system logging remote configure

S.No	Command Name	Description	Type and Description
1	save	Save remoteLogging configuration changes.	
2	exit	Save remote logging configuration changes and exit current mode.	
3	cancel	Roll back remote logging configuration changes.	
4	log_identifier	Set the log identifier prefixed to both, e-mail and Syslog messages.	String
5	email_logs_enable	Set whether or not system emails scheduled logs.	Boolean choice
6	email_server	Set options for emailing of logs.	String
7	smtp_port	The SMTP port of the e-mail server.	Port number
8	return_email_address	Set email address SMTP server replies are sent.	String
9	send_to_email_addresses	Set email address where logs and alerts will be sent.	String
10	send_to_email_addresses2	Set email address where logs and alerts will be sent.	String
11	send_to_email_addresses3	Set email address where logs and alerts will be sent.	String
12	smtp_auth	Set SMTP authentication details.	
13	smtp_auth type	Set SMTP authentication types.	SMTP Authentication Types.
14	smtp_auth username	Set SMTP authentication username (for plain and CRAM- MD5 auth).	String
15	smtp_auth password	Set SMTP authentication password (for plain and CRAM- MD5 auth).	String

S.No	Command Name	Description	Type and Description
16	Tls_Enable	Enable Tls support (for plain and CRAM-MD5 auth).	Boolean choice
17	identd_from_smtp_server_enable	Enable/Diable to identd from smtp server.	Boolean choice
18	schedule	Set schedule for sending log by email.	
19	schedule unit	Set schedule unit.	Schedule Unit Types.
20	schedule day	Set schedule day.	Schedule Day Types.
21	schedule time	Set schedule time.	Schedule Time Units Types.
22	schedule meridiem	Set schedule meridiem.	Schedule Meridiem Types.
23	syslog_server	syslog	
24	syslog_server server_name1	server1	
25	syslog_server server_name2	server2	
26	syslog_server server_name3	server3	
27	syslog_server server_name4	server4	
28	syslog_server server_name5	server5	
29	syslog_server server_name6	server6	
30	syslog_server server_name7	server7	
31	syslog_server server_name8	server8	
32	syslog_server server_name1 enable	Boolean Choice Y/N	Boolean choice
33	syslog_server server_name1 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
34	syslog_server server_name1 severity	Set Syslog severity.	syslog server severity types
35	syslog_server server_name1 facility	Set Syslog facility.	syslog server facility ID types
36	syslog_server server_name2 enable	Boolean Choice Y/N	Boolean choice
37	syslog_server server_name2 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
38	syslog_server server_name2 severity	Set Syslog severity.	syslog server severity types

S.No	Command Name	Description	Type and Description
39	syslog_server server_name2 facility	Set Syslog facility.	syslog server facility ID types
40	syslog_server server_name3 enable	Boolean Choice Y/N	Boolean choice
41	syslog_server server_name3 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
42	syslog_server server_name3 severity	Set Syslog severity.	syslog server severity types
43	syslog_server server_name3 facility	Set Syslog facility.	syslog server facility ID types
44	syslog_server server_name4 enable	Boolean Choice Y/N	Boolean choice
45	syslog_server server_name4 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
46	syslog_server server_name4 severity	Set Syslog severity.	syslog server severity types
47	syslog_server server_name4 facility	Set Syslog facility.	syslog server facility ID types
48	syslog_server server_name5 enable	Boolean Choice Y/N	Boolean choice
49	syslog_server server_name5 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
50	syslog_server server_name5 severity	Set Syslog severity.	syslog server severity types
51	syslog_server server_name5 facility	Set Syslog facility.	syslog server facility ID types
52	syslog_server server_name6 enable	Boolean Choice Y/N	Boolean choice
53	syslog_server server_name6 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
54	syslog_server server_name6 severity	Set Syslog severity.	syslog server severity types
55	syslog_server server_name6 facility	Set Syslog facility.	syslog server facility ID types
56	syslog_server server_name7 enable	Boolean Choice Y/N	Boolean choice

S.No	Command Name	Description	Type and Description
57	syslog_server server_name7 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
58	syslog_server server_name7 severity	Set Syslog severity.	syslog server severity types
59	syslog_server server_name7 facility	Set Syslog facility.	syslog server facility ID types
60	syslog_server server_name8 enable	Boolean Choice Y/N	Boolean choice
61	syslog_server server_name8 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
62	syslog_server server_name8 severity	Set Syslog severity.	syslog server severity types
63	syslog_server server_name8 facility	Set Syslog facility.	syslog server facility ID types

## 8.9 system logging ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv6 logging configuration changes.	
2	exit	Save ipv6 logging configuration changes and exit current mode.	
3	cancel	Roll back ipv6 logging configuration changes.	
4	lan_wan_accept_enable	Enable/Disable logging for the LAN to WAN Accept packets	Boolean choice
5	lan_wan_drop_enable	Enable/Disable logging for the LAN to WAN Dropped packets	Boolean choice
6	wan_lan_accept_enable	Enable/Disable logging for the WAN to LAN Accept packets	Boolean choice
7	wan_lan_drop_enable	Enable/Disable logging for the WAN to LAN Dropped packets	Boolean choice



## 8.10 system logging SMS configure

S.No	Command Name	Description	Type and Description
1	save	Save SMS logging configuration changes	
2	exit	Save SMS logging settings and exit current mode	
3	cancel	Roll back SMS logging configuration changes	
4	enter_mobile_num	Enter mobile number on which SMS will be sent	enter mobile number of 11 or 12 digits
5	wan_up/down	Enable this option to get WAN UP/Down event based SMS	Boolean choice
6	vpn_connect/disconnect	Enable this option to get VPN connect/disconnect event based SMS	Boolean choice
7	cpu_memory_usage_reaches_80%	Enable this option to get event based SMS when CPU/Memory usage reached to 80%	Boolean choice

## 8.11 system Radius-Settings

S.No	Command Name	Description	Type and Description
1	save	Save RADIUS configuration changes.	
2	exit	Save RADIUS configuration changes and exit current mode.	
3	cancel	Roll back configuration changes	
4	primary-radius-server	Set Primary RADIUS server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	secondary-radius-server	Set Secondary RADIUS server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	optional-radius-server	Set Optional RADIUS server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	primary-server-authentication-port	Set Primary RADIUS server port.	Port number

S.No	Command Name	Description	Type and Description
8	secondary-server-authentication-port	Set Secondary RADIUS server port.	Port number
9	optional-server-authentication-port	Set Optional RADIUS server port.	Port number
10	primary-server-secret	Set Primary RADIUS server secret.	String
11	secondary-server-secret	Set Secondary RADIUS server secret.	String
12	optional-server-secret	Set Optional RADIUS server secret.	String
13	primary-server-timeout	Set primary server connection timeout.	radius server connection timeout in seconds
14	secondary-server-timeout	Set secondary server connection timeout.	radius server connection timeout in seconds
15	optional-server-timeout	Set optional server connection timeout.	radius server connection timeout in seconds
16	primary-server-retries	Set primary server connection retry attempts.	radius server retries attempts.
17	secondary-server-retries	Set secondary server connection retry attempts.	radius server retries attempts.
18	optional-server-retries	Set optional server connection retry attempts.	radius server retries attempts.
19	serverCheck	Check the reachability of configured servers.	

## 8.12 system remote\_management https configure

S.No	Command Name	Description	Type and Description
1	save	save access Management changes for https.	
2	exit	Save access Management changes for https and exit current mode.	
3	cancel	Roll back Remote Mgmt changes.	
4	enable	Enable/disable remote mgmt over https.	Boolean choice
5	type	Enable/disable remote mgmt over https.	Unsigned integer
6	from_address	Set the starting IP in case of range, and the IP to be allowed access in case of granting access to a particular machine	IP address AAA.BBB.CCC.DDD where each part is in the range 0- 255

S.No	Command Name	Description	Type and Description
7	end_address	Set the Ending IP in case of range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0- 255
8	port	Set the port you want to use for HTTP.	Unsigned integer
9	enable_remote_snmp	Enable/disable remote snmp.	Boolean choice

### 8.13 system remote\_management telnet configure

S.No	Command Name	Description	Type and Description
1	save	save access Management changes for telnet.	
2	exit	Save access Management changes for telnet and exit current mode.	
3	cancel	Roll back Remote Mgmt changes.	
4	enable	Enable/disable remote mgmt over telnet.	Boolean choice
5	type	The kind of access you want to allow.	Unsigned integer
6	from_address	Set the starting IP in case of range, and the IP to be allowed access in case of granting access to a particular machine	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	to_address	Set the Ending IP in case of range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

### 8.14 system snmp trap configure <agent\_ip>

S.No	Command Name	Description	Type and Description
1	<agent_ip>	SNMP trap configuration mode.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	save	Save SNMP trap configuration changes.	
3	exit	Save SNMP trap configuration changes and exit current mode.	
4	cancel	Roll back snmp configuration changes.	

S.No	Command Name	Description	Type and Description
5	agent	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	snmp_version	Snmp Version v1/v2/v3	snmp version
7	port	SNMP trap port the trap messages will be sent to.	Port number
8	community	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community	String

## 8.15 system snmp trap delete <agent\_ip>

S.No	Command Name	Description	Type and Description
1	<agent_ip>	Delete a SNMP trap configuration.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

## 8.16 system snmp users configure <user>

S.No	Command Name	Description	Type and Description
1	<user>	SNMP v3 User list configuration changes	snmpv3users list user type
2	save	Save SNMP trap configuration changes.	
3	exit	save SNMP v3 Users configuration changes and exit current mode.	
4	cancel	Roll back SNMP v3 Users configuration changes.	
5	security_level	authentication and privacy settings .	snmp security level type for snmpv3users list
6	authentication_algo	choose between MD5 or SHA authentication	snmpv3users list authentication algorithm type
7	privacy_algorithm	DES-56 privacy is available for the authentication negotiation	snmpv3users list privacy algorithm type
8	authentication_password	shared authentication password with the SNMPv3 user.	String
9	privacy_password	shared privacy password with the SNMPv3 user	String

## 8.17 system snmp sys configure

S.No	Command Name	Description	Type and Description
1	save	Save SNMP system configuration changes.	
2	cancel	Roll back snmp configuration changes.	
3	exit	Save SNMP system configuration changes and exit current mode.	
4	sys-contact	Set system contact information.	String
5	sys-location	Set system location information.	String
6	sys-name	Set system name information.	String

## 8.18 system snmp access add

S.No	Command Name	Description	Type and Description
1	save	Save SNMP access control configuration changes.	
2	exit	Save SNMP access configuration changes and exit current mode.	
3	cancel	Roll back snmp configuration changes.	
4	ip_iddress	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
5	subnet_mask	The network mask used to determine the list of allowed SNMP managers. To allow any IP on the network to manager the device enter 255.255.255.0. For a specific host, enter 255.255.255.255. To allow global access, enter 0.0.0.0.	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
6	accessType	SNMP trap port the trap messages will be sent to.	access type either read only or read write
7	community	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community	String

## 8.19 system snmp access edit <rowid>

S.No	Command Name	Description	Type and Description
1	<rowid>	snmp configuration mode	Unsigned integer
2	save	Save SNMP access control configuration changes.	
3	exit	Save SNMP access configuration changes and exit current mode.	
4	cancel	Roll back snmp configuration changes.	
5	ip_iddress	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
6	subnet_mask	The network mask used to determine the list of allowed SNMP managers. To allow any IP on the network to manager the device enter 255.255.255.0. For a specific host, enter 255.255.255.255. To allow global access, enter 0.0.0.0.	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
7	accessType	SNMP trap port the trap messages will be sent to.	access type either read only or read write
8	community	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community	String

## 8.20 system snmp access delete <rowid>

S.No	Command Name	Description	Type and Description
1	<rowid>	SNMP access configuration mode.	Unsigned integer

## 8.21 system switch\_settings power\_saving configure

S.No	Command Name	Description	Type and Description
1	save	Save powerMode configuration changes.	

S.No	Command Name	Description	Type and Description
2	exit	Save power mode configuration changes and exit current mode.	
3	cancel	Roll back content Filtering over mode configuration changes.	
4	link_status	Enable/Disable Link status	Boolean choice
5	cable_length	enable/disable Cable Length	Boolean choice

## 8.22 system switch\_settings jumbo\_frame configure

S.No	Command Name	Description	Type and Description
1	save	Save jumbo frame configuration changes.	
2	exit	Save jumbo frame configuration changes and exit current mode.	
3	cancel	Roll back jumbo frame configuration changes.	
4	jumbo_frame	Enable/Disable jumbo frame	Boolean choice

## 8.23 system admin\_setting configure

S.No	Command Name	Description	Type and Description
1	save	Save system admin changes.	
2	exit	Save configuration changes and exit current mode.	
3	cancel	Roll back admin configuration changes.	
4	System_name		String

## 8.24 system session\_setting configure

S.No	Command Name	Description	Type and Description
1	save	Save session logout changes.	
2	exit	Save configuration changes and exit current mode.	
3	cancel	Roll back admin configuration changes.	
4	admin.timeout		session timeout range
5	guest.timeout		session timeout range

## 8.25 system time configure

S.No	Command Name	Description	Type and Description
1	save	Save time configuration changes.	
2	exit	Save time configuration changes and current mode.	
3	cancel	Roll back time configuration changes.	
4	time_zone	Specify timezone	Timezones
5	enable_daylight_saving	Specify whether you want to enable daylight saving	Boolean choice
6	configure_ntp_servers	Specify whether to use ntp servers or user will set date and time	Boolean choice
7	use_default_servers	Specify whether to use system default NTP servers or custom NTP servers.	Boolean choice
8	primary_ntp_server	Set Primary NTP server.	String
9	secondary_ntp_server	Set Secondary NTP server	String
10	ntp_year	Set year for the date	Year
11	ntp_month	Set month for the date	Month in the format MM(01-12)
12	ntp_day	Set Day for the date	Day in the format DD(01-31)
13	ntp_hour	Set hour for the date	HH(00-23) using 24 hour clock
14	ntp_minutes	Set minutes for the date	minute in the format MM(00-59)
15	ntp_seconds	Set seconds for the date	Second in the format SS(00-59)
16	ntp_sync_interval	Set sync interval (in minutes)	Unsigned integer

## 8.26 system traffic\_meter configure

S.No	Command Name	Description	Type and Description
1	save	Save traffic meter configuration changes.	
2	exit	Save traffic meter configuration changes and exit current mode.	
3	cancel	Roll back traffic meter configuration changes.	
4	enable	Enable/Disable the traffic meter status	Boolean choice
5	limit_type	Set traffic Limit Type 0(No limit), 1(Download only), 2(Both Directions)	traffic meter types
6	monthly_limit	Set the monthly limit value of the traffic meter	Unsigned integer



S.No	Command Name	Description	Type and Description
7	increase_limit_enable	Enable/Disable status of increase limit of the traffic meter option	Boolean choice
8	increase_limit_by	Set the value to increase limit of the traffic meter	Unsigned integer
9	counter	set traffic counter as either specific time or restart counter now	traffic counter type
10	time_hour	set hours for restart time	HH(00-23) using 24 hour clock
11	time_minute	set minutes for restart time	minute in the format MM(00-59)
12	day_of_month	set day of month	Calendar day of month
13	send_email_report	Enable/Disable send email report	Boolean choice
14	block_type	Set block Traffic type 0(block all traffic) 1(block all traffic except email)	block traffic type.
15	send_email_alert	Enable/Disable send email alert	Boolean choice

## 8.27 system usb usb1 configure

S.No	Command Name	Description	Type and Description
1	save	Save Configurable WAN settings.	
2	exit	Save configurable WAN settings and exit current mode.	
3	cancel	Roll back Configurable WAN settings changes.	
4	enable	Enable USB1	Boolean choice
5	printer_enable	Enable printer usb	Boolean choice
6	Storage_enable	Enable Storage USB	Boolean choice
7	usb_type	Selects the USB type 3G_USB_ADAPTOR/USB_Disc	usb device type

## 8.28 system usb usb2 configure

S.No	Command Name	Description	Type and Description
1	save	Save USB1 Settings settings.	
2	exit	Save USB2 settings and exit current mode.	

S.No	Command Name	Description	Type and Description
3	cancel	Roll back Configurable WAN settings changes.	
4	enable	Enable USB2.	Boolean choice
5	printer_enable	Enable printer.	Boolean choice
6	Storage_enable	Enable USB2.	Boolean choice
7	usb_type	Selects the USB type 3G_USB_ADAPTOR/USB_Di sc.	usb device type

## 8.29 system usb shareport\_vlan configure <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	SharePort on vlan configuration.	Unsigned integer
2	save	Save SharePort on vlan settings.	
3	exit	Save shareport on vlan settings and exit current mode.	
4	cancel	Roll back Configurable VLAN changes.	
5	printer_sharing	Enable printer	Boolean choice
6	storage_sharing	Enable USB2	Boolean choice

## 8.30 system group add

S.No	Command Name	Description	Type and Description
1	save	Save system group configuration changes.	
2	exit	Save system group configuration changes and exit current mode.	
3	cancel	Roll back system group configuration changes.	
4	groupname	Enter the Group Name here	Only AtoZ, atoz and 0to9 characters are allowed
5	description	Enter a brief description of the group here	String
6	userType	Select the user type for the group.	User Type available.
7	Privilege_Type	Select the privilege type for the group.	

S.No	Command Name	Description	Type and Description
8	Privilege_Type sslvpn	Adds sslvpn privilege to the group	Boolean choice
9	Privilege_Type L2TP	Adds L2TP privilege to the group	Boolean choice
10	Privilege_Type PPTP	Adds PPTP privilege to the group	Boolean choice
11	Privilege_Type Xauth	Adds Xauth privilege to the group	Boolean choice
12	Privilege_Type OpenVPN	Adds open vpn privilege to the group	Boolean choice
13	grouptimeOut	Enter the time out for the group	idle timeout value for user.

### 8.31 system group edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	system groups edit mode.	Unsigned integer
2	save	Save system group configuration changes.	
3	exit	Save system group configuration changes and exit current mode.	
4	cancel	Roll back system group configuration changes.	
5	description	Enter a brief description of the group here	String
6	grouptimeOut	Enter the new time out for the group	idle timeout value for user.
7	userType	Select the user type for the group.	User Type available.
8	Privilege_Type	Select the privilege type for the group.	
9	Privilege_Type sslvpn	Adds sslvpn privilege to the group	Boolean choice
10	Privilege_Type L2TP	Adds L2TP privilege to the group	Boolean choice
11	Privilege_Type PPTP	Adds PPTP privilege to the group	Boolean choice
12	Privilege_Type Xauth	Adds Xauth privilege to the group	Boolean choice
13	Privilege_Type OpenVPN	Adds open vpn privilege to the group	Boolean choice

## 8.32 system group delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	System groups delete mode.	Unsigned integer

## 8.33 system users add

S.No	Command Name	Description	Type and Description
1	save	Save system user configuration changes.	
2	exit	Save system user configuration changes and exit current mode.	
3	cancel	Roll back system user configuration changes.	
4	username	Enter the username here	Only AtoZ, atoz and 0to9 characters are allowed
5	FirstName	Enter the user's first name here	String
6	LastName	Enter the user's last name here	String
7	password	Enter the password here	String
8	password_confirm	Re-Enter the password here	String
9	groupname	Enter the groupname here	String
10	enable_change_password	Enable/Disable change password for captive portal user	Boolean choice

## 8.34 system users edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	system users edit mode.	Unsigned integer
2	save	Save system user configuration changes.	
3	exit	Save system user configuration changes and exit current mode.	
4	cancel	Roll back system user configuration changes.	
5	FirstName	Enter the user's first name here	String
6	LastName	Enter the user's last name here	String
7	change_password	Change user's password	String

S.No	Command Name	Description	Type and Description
			String String
8	enable_change_password	Enable/Disable change password for captive portal user	Boolean choice
9	groupname	Enter the groupname here	String

### 8.35 system users delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	system users delete mode.	Unsigned integer

### 8.36 system group groupaccesscontrol configure <group\_id>

S.No	Command Name	Description	Type and Description
1	<group_id>	group access control configuration	Unsigned integer
2	save	Save group access control configuration changes.	
3	exit	Save group access control configuration changes and exit current mode.	
4	cancel	Roll back group access control configuration changes.	
5	deny_login	deny login	Boolean choice
6	deny_login_wan	deny login wan	Boolean choice
7	allow_login_from_defined_ips	login from ip	Boolean choice
8	allow_login_from_defined_browsers	login from browser	Boolean choice

### 8.37 system group access\_control\_browser add

S.No	Command Name	Description	Type and Description
1	save	Save group access control browser configuration changes.	
2	exit	Save group access control browser configuration	

S.No	Command Name	Description	Type and Description
		changes and exit current mode.	
3	cancel	Roll back group access control browser configuration changes.	
4	group_id	group id	Unsigned integer
5	browser_name	browser name	Supported browsers

### 8.38 system group access\_control\_browser delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete a browser from Access Control browsers list.	Unsigned integer

### 8.39 system group access\_control\_ip add

S.No	Command Name	Description	Type and Description
1	save	Save group access control ip configuration changes.	
2	exit	Save group access control ip configuration changes and exit current mode.	
3	cancel	Roll back group access control ip configuration changes.	
4	group_id	group id	Unsigned integer
5	address_type	address type	source address type for users ip policy
6	source_address	Set the source address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	mask_length	Set the source network mask length	number in range of 1 to 32

## 8.40 system group access\_control\_ip delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete an ip from Access Control ips list.	Unsigned integer

## Chapter 9. Configuration commands under branch UTIL

### 9.1 util system\_check ping <ip\_address>

S.No	Command Name	Description	Type and Description
1	<ip_address>	Ping an Internet Address.	String

### 9.2 util system\_check dns\_lookup <dns>

S.No	Command Name	Description	Type and Description
1	<dns>	To retrieve the IP address of a Web, FTP, Mail or any other Server on the Internet	String

### 9.3 util system\_check traceroute <ip\_address>

S.No	Command Name	Description	Type and Description
1	<ip_address>	Displays all the routers present between the destination IP address and this router.	String

### 9.4 util system\_check capturePackets start <interface>

S.No	Command Name	Description	Type and Description
1	<interface>	Starts the packet capture.	String

### 9.5 util system\_check capturePackets download <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Download the packet capture to the host machine.	FileName string IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

### 9.6 util dbglog\_download <fileName> <ipAddr>

S.No	Command Name	Description	Type and Description
1	<fileName> <ipAddr>	Download Dbglogs to the host machine	FileName string IP address AAA.BBB.CCC.DDD



S.No	Command Name	Description	Type and Description
			where each part is in the range 0-255

### 9.7 util usb\_test <ipAddr> <fileName>

S.No	Command Name	Description	Type and Description
1	<ipAddr> <fileName>	To test the USB.	String FileName string

### 9.8 util enable\_auto\_backup <status>

S.No	Command Name	Description	Type and Description
1	<status>	Enable/Disable Auto Backup support.	Boolean choice.

### 9.9 util enable\_config\_encryp <status>

S.No	Command Name	Description	Type and Description
1	<status>	Enable/Disable Configuration encryption support.	Boolean choice

### 9.10 util watchdog\_disable <status>

S.No	Command Name	Description	Type and Description
1	<status>	Disable/Enable watchdog timer.	Boolean choice

# Chapter 10. Configuration commands under branch LICENSE

## 10.1 license list

S.No	Command Name	Description	Type and Description
1	list	List all licenses configured on the device	
2	activate	Activate a license on the device	
3	trial_activate	Activate trial period of 90 days to use WCF.	
4	trial_activate_status	displays the details of free trial expiry in days.	

## 10.2 license activate <activationKey>

S.No	Command Name	Description	Type and Description
1	<activationKey>	activate a license on the device.	Takes a string value that has only AtoZ, atoz and 0to9 characters only
2	list	List all licenses configured on the device	
3	activate	Activate a license on the device	
4	trial_activate	Activate trial period of 90 days to use WCF.	
5	trial_activate_status	displays the details of free trial expiry in days.	

## 10.3 license trial\_activate

S.No	Command Name	Description	Type and Description
1	list	List all licenses configured on the device	
2	activate	Activate a license on the device	
3	trial_activate	Activate trial period of 90 days to use WCF.	
4	trial_activate_status	displays the details of free trial expiry in days.	

## 10.4 license trial\_activate\_status

S.No	Command Name	Description	Type and Description
1	list	List all licenses configured on the device	
2	activate	Activate a license on the device	
3	trial_activate	Activate trial period of 90 days to use WCF.	
4	trial_activate_status	displays the details of free trial expiry in days.	

# Chapter 11. Configuration commands under branch NET

## 11.1 net ipv6\_tunnel six\_to\_four configure

S.No	Command Name	Description	Type and Description
1	save	Save sixToFour Tunnel configuration changes.	
2	exit	Save sixToFour Tunnel configuration changes and exit current mode.	
3	cancel	Roll back sixToFourTunnel configuration changes.	
4	automatic_tunneling_enable	enable/disable automatic tunneling which will allow traffic from a LAN IPv6 network to be tunneled through a WAN IPv4 network to reach an IPV6 network.	Boolean choice

## 11.2 net bandwidth profile enable <enable>

S.No	Command Name	Description	Type and Description
1	<enable>	It allows to enable/disable bandwidth profiles.	Boolean choice

## 11.3 net bandwidth profile add

S.No	Command Name	Description	Type and Description
1	save	Save bandwidth profile configuration changes.	
2	exit	Save bandwidth Profile configuration changes and exit current mode.	
3	cancel	Roll back bandwidth Profile configuration changes.	
4	name	Unique Profile Name.	Only AtoZ, atoz and 0to9 characters are allowed
5	policytype	Policy Type, either Inbound or Outbound.	bandwidth policy type
6	Profiletype	Profile Type, either Priority or Rate.	bandwidth profile type
7	priority	Priority.	bandwidth priority type

S.No	Command Name	Description	Type and Description
8	minimum_rate	Minimum Bandwidth provided by user.	Minimum bandwidth rate 0- Max bandwidth Kbps
9	maximum_rate	Maximum Bandwidth provided by user.	Maximum bandwidth rate 100-100000 Kbps
10	Interface	Enter WAN interface(WAN1/WAN2) for Outbund Policy and LAN/VLAN (Use show net bandwidth profile interface_list command to see list)interface for Inbound Bandwidth Profile	String

### 11.4 net bandwidth profile edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to edit a bandwidth profile.	Unsigned integer
2	save	Save bandwidth profile configuration changes.	
3	exit	Save bandwidth Profile configuration changes and exit current mode.	
4	cancel	Roll back bandwidth Profile configuration changes.	
5	name	Unique Profile Name.	Only AtoZ, atoz and 0to9 characters are allowed.
6	policytype	Policy Type, either Inbound or Outbound.	bandwidth policy type
7	Profiletype	Profile Type, either Priority or Rate.	bandwidth profile type
8	priority	Priority.	bandwidth priority type
9	minimum_rate	Minimum Bandwidth provided by user.	Minimum bandwidth rate 0- Max bandwidth Kbps
10	maximum_rate	Maximum Bandwidth provided by user.	Maximum bandwidth rate 100-100000 Kbps
11	Interface	Enter WAN interface(WAN1/WAN2) for Outbund Policy and LAN/VLAN (Use show net bandwidth profile interface_list command to see	String

S.No	Command Name	Description	Type and Description
		list)interface for Inbound Bandwidth Profile.	

## 11.5 net bandwidth profile delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to delete a bandwidth profile.	Unsigned integer

## 11.6 net bandwidth traffic\_selector add

S.No	Command Name	Description	Type and Description
1	save	Save Traffic Selector configuration changes.	
2	exit	Save Traffic Selector configuration changes and exit current mode.	
3	cancel	Roll back Traffic Selector configuration changes.	
4	profile_name	Profile Name.	String
5	service_name	Service Name.	String
6	match_type	IP /MAC Address	traffic selector match type
7	ip_address	IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	subnet_mask	Subnet Mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	BSSID	Enter BSSID or vapname (Use show net bandwidth traffic_selector BSSID for Available BSSID).	String
10	mac_address	MAC Address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
11	port_name	Port Name	traffic selectors Port types
12	vlan_id	Vlan ID	Unsigned integer

## 11.7 net bandwidth traffic\_selector edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to edit a traffic selector for a bandwidth profile.	Unsigned integer
2	save	Save Traffic Selector configuration changes.	
3	exit	Save Traffic Selector configuration changes and exit current mode.	
4	cancel	Roll back Traffic Selector configuration changes.	
5	profile_name	Profile Name.	String
6	service_name	Service Name.	String
7	match_type	IP /MAC Address	traffic selector match type
8	ip_address	IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	subnet_mask	Subnet Mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	BSSID	Enter BSSID or vapname (Use show net bandwidth traffic_selector BSSID for Available BSSID).	String
11	mac_address	MAC Address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
12	port_name	Port Name	traffic selectors Port types
13	vlan_id	Vlan ID	Unsigned integer

## 11.8 net bandwidth traffic\_selector delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to delete a traffic selector for a bandwidth profile.	Unsigned integer

## 11.9 net ddns wan1 configure

S.No	Command Name	Description	Type and Description
1	save	Save DDNS configuration changes.	
2	exit	Save DDNS configuration changes and exit current mode.	
3	cancel	Roll back DDNS configuration changes.	
4	ddnsService	Enable or disable Dyn dns to provide Dynamic DNS services available	Dynamic DNS Services available.
5	server	Set Dynamic DNS Server.	String
6	username	Set username.	String
7	password	Set Password.	String
8	hostname	Set Hostname.	String
9	zonename	Set Zonename.	String
10	type	Set DDNS Type.	Dynamic DNS Type available.
11	wild_flag_enable	Enable / Disable using wild cards.	Boolean choice
12	force_update_interval	Set ForceUpdate Interval.	ddns update interval in days
13	use_external_nat_ip	Enable / Disable this for using external (NAT router's) IP address or not.	Boolean choice
14	url	Set Custom DDNS Service Url.	String
15	add_option	Set Custom Service additional options.	String, ' character is not supported;
16	key	Upload key for Dynamic Update DDNS Service Authentication.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.10 net ddns wan2 configure

S.No	Command Name	Description	Type and Description
1	save	Save DDNS configuration changes.	
2	exit	Save DDNS configuration changes and exit current mode.	
3	cancel	Roll back DDNS configuration changes.	



S.No	Command Name	Description	Type and Description
4	ddnsService	Enable or disable Dyndns to provide Dynamic DNS services available	Dynamic DNS Services available.
5	server	Set Dynamic DNS Server.	String
6	username	Set username.	String
7	password	Set Password.	String
8	hostname	Set Hostname.	String
9	zonename	Set Zonename.	String
10	type	Set DDNS Type.	Dynamic DNS Type available.
11	wild_flag_enable	Enable / Disable using wild cards.	Boolean choice
12	force_update_interval	Set ForceUpdate Interval.	ddns update interval in days
13	use_external_nat_ip	Enable / Disable this for using external (NAT router's) IP address or not.	Boolean choice
14	url	Set Custom DDNS Service Url.	String
15	add_option	Set Custom Service additional options.	String, ' character is not supported;
16	key	Upload key for Dynamic Update DDNS Service Authentication.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.11 net ddns wan3 configure

S.No	Command Name	Description	Type and Description
1	save	Save DDNS configuration changes.	
2	exit	Save DDNS configuration changes and exit current mode.	
3	cancel	Roll back DDNS configuration changes.	
4	ddnsService	Enable or disable Dyndns to provide Dynamic DNS services available	Dynamic DNS Services available.
5	server	Set Dynamic DNS Server.	String
6	username	Set username.	String
7	password	Set Password.	String
8	hostname	Set Hostname.	String
9	zonename	Set Zonename.	String
10	type	Set DDNS Type.	Dynamic DNS Type available.

S.No	Command Name	Description	Type and Description
11	wild_flag_enable	Enable / Disable using wild cards.	Boolean choice
12	force_update_interval	Set ForceUpdate Interval.	ddns update interval in days
13	use_external_nat_ip	Enable / Disable this for using external (NAT router's) IP address or not.	Boolean choice
14	url	Set Custom DDNS Service Url.	String
15	add_option	Set Custom Service additional options.	String, ' character is not supported;
16	key	Upload key for Dynamic Update DDNS Service Authentication.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.12 net lan dhcp reserved\_ip configure <mac\_address>

S.No	Command Name	Description	Type and Description
1	<mac_address>	DHCP Reserved IPs add/edit mode.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
2	save	Save DHCP Reserved IPs configuration changes.	
3	exit	Save DHCP Reserved IPs configuration changes and exit current mode.	
4	cancel	Roll back DHCP Reserved IPs configuration changes.	
5	ip_address	Set IP Address to be reserved	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	computer_name	Specify a unique name	String
7	Association	Select to Associate with IP / MAC Binding	Boolean choice
8	Log_Dropped_Packets	Displays logging option for the dropped packets.	Boolean choice

### 11.13 net lan dhcp reserved\_ip delete <mac\_address>

S.No	Command Name	Description	Type and Description
1	<mac_address>	Deletes a specific reserved ip entry.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

### 11.14 net dmz dhcp reserved\_ip configure <mac\_address>

S.No	Command Name	Description	Type and Description
1	<mac_address>	DHCP Reserved IPs add/edit mode.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
2	save	Save DHCP Reserved IPs configuration changes.	
3	exit	Save DHCP Reserved IPs configuration changes and exit current mode.	
4	cancel	Roll back DHCP Reserved IPs configuration changes.	
5	ip_address	Set IP Address to be reserved	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

### 11.15 net dmz dhcp reserved\_ip delete <mac\_address>

S.No	Command Name	Description	Type and Description
1	<mac_address>	Delete a specific reserved ip entry.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

### 11.16 net ethernet configure <interface\_name>

S.No	Command Name	Description	Type and Description
1	<interface_name>	Ethernet configuration mode.	String
2	save	Save ethernet configuration changes	
3	exit	Save ethernet configuration changes and exit current mode.	

S.No	Command Name	Description	Type and Description
4	cancel	Roll back configuration changes.	
5	vlan-enable	Enable/Disable VLAN for this interface.	Boolean choice
6	native-vlan	Enable/Disable native VLAN status.	Boolean choice
7	vlanid	Set VLAN Id.	Unsigned integer

## 11.17 net lan ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save LAN configuration changes.	
2	exit	Save LAN configuration changes and exit current mode.	
3	cancel	Roll back LAN configuration changes.	
4	static	Configure LAN Settings.	
5	static address	Set system LAN IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	static subnet_mask	Set system LAN subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	dhcp	Configure DHCP Settings.	
8	dhcp mode	Set dhcp mode.	dhcpv4 modes
9	dhcp start_address	Set dhcp servers start address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	dhcp end_address	Set dhcp servers end address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	dhcp default_gw	Set dhcp default gateway.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	dhcp primary_dns	Set primary dns server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	dhcp secondary_dns	Set secondary dns server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
14	dhcp wins_server	Set Wins Server address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
15	dhcp lease_time	Set system Lease Time.	number in range of 1 to 262800
16	dhcp domain_name	Set dhcp domain name.	String
17	dhcp relay_gateway	Set dhcp relays gateway address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
18	dns	Configure DNS Settings.	
19	dns host_name	Configure DNS Settings.	
20	dns host_name mapping	Configure DNS Host NameMapping.	
21	dns host_name mapping 1	Configure DNS Host NameMapping for 1st row.	
22	dns host_name mapping 2	Configure DNS Host NameMapping for 2nd Row.	
23	dns host_name mapping 3	Configure DNS Host NameMapping for 3rd row.	
24	dns host_name mapping 4	Configure DNS Host NameMapping for 4th row.	
25	dns host_name mapping 5	Configure DNS Host NameMapping for 5th row.	
26	dns host_name mapping 6	Configure DNS Host NameMapping for 6th row.	
27	dns host_name mapping 7	Configure DNS Host NameMapping for 7th row.	
28	dns host_name mapping 8	Configure DNS Host NameMapping for 8th row.	
29	dns host_name mapping 1 host_name	Set Host Name.	String
30	dns host_name mapping 1 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
31	dns host_name mapping 2 host_name	Set Host Name.	String
32	dns host_name mapping 2 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
33	dns host_name mapping 3 host_name	Set Host Name.	String
34	dns host_name mapping 3 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
35	dns host_name mapping 4 host_name	Set Host Name.	String

S.No	Command Name	Description	Type and Description
36	dns host_name mapping 4 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
37	dns host_name mapping 5 host_name	Set Host Name.	String
38	dns host_name mapping 5 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
39	dns host_name mapping 6 host_name	Set Host Name.	String
40	dns host_name mapping 6 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
41	dns host_name mapping 7 host_name	Set Host Name.	String
42	dns host_name mapping 7 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
43	dns host_name mapping 8 host_name	Set Host Name.	String
44	dns host_name mapping 8 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
45	proxy	Configure the LAN Proxies	
46	proxy dns_enable	Enable/Disable dns proxy	Boolean choice

## 11.18 net lan ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Save LAN configuration changes.	
2	exit	Save LAN configuration changes and exit current mode.	
3	cancel	Roll back LAN configuration changes.	
4	static	Set system LAN Settings.	
5	static address	Set system LAN IP address.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
6	static prefix_value	Prefix length	Unsigned integer
7	dhcp	Set system LAN Settings.	
8	dhcp server_enable	Set dhcpv6 server status	Boolean choice

S.No	Command Name	Description	Type and Description
9	dhcp mode	DHCPv6 Mode	dhcpv6 modes
10	dhcp domain_name	dhcp server domain name	String
11	dhcp server_preference	server preference number	Unsigned integer
12	dhcp dns_type	dns server type	dhcpv6 dns server types
13	dhcp primary_dns	primary dns server	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
14	dhcp secondary_dns	Secondary dns server	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
15	dhcp rebind_time	Rebind time	number in range of 0 to 604800

## 11.19 net lan ipv6 pool configure <ipv6PoolStartAddr>

S.No	Command Name	Description	Type and Description
1	<ipv6PoolStartAddr>	IPv6 LAN configuration add/edit mode.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
2	save	Save LAN configuration changes.	
3	exit	Save LAN configuration changes and exit current mode.	
4	cancel	Roll back LAN configuration changes.	
5	start_address	Set dhcpv6 start IP address.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
6	end_address	Set dhcpv6 end IP address.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
7	prefix_value	Prefix length	Unsigned integer

## 11.20 net lan ipv6 pool delete <ipv6PoolStartAddr>

S.No	Command Name	Description	Type and Description
1	<ipv6PoolStartAddr>	IPv6 LAN configuration delete.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

## 11.21 net igmp configure

S.No	Command Name	Description	Type and Description
1	save	Save igmp settings	
2	exit	Save igmp settings and exit current mode	
3	cancel	Roll back igmp settings changes	
4	Enable	Specify the igmp proxy should enable or disable	Boolean choice
5	UpStreamInterface_WAN	This command is used to select WAN upstream interface for WAN	WAN interface type WAN-DHCP/WAN-PPTP/WAN-L2TP

## 11.22 net igmp snooping configure

S.No	Command Name	Description	Type and Description
1	save	Save igmp snooping settings	
2	exit	Save igmp snooping settings and exit current mode	
3	cancel	Roll back igmp snooping settings changes	
4	Enable	Specify the igmp snooping should enable or disable	Boolean choice

## 11.23 net igmp portmap configure <vlanId>

S.No	Command Name	Description	Type and Description
1	<vlanId>	Specify igmp port map configuration	Number in the range 1-4095
2	save	Save igmp portmap settings	
3	exit	Save igmp portmap settings and exit current mode	



S.No	Command Name	Description	Type and Description
4	cancel	Roll back igmp portmap settings changes	
5	portmembership	Specify the igmp port membership to the selected vlan	Port number(s) a,b,c where each part is a valid port number in the range [1-8]

## 11.24 net intel\_Amt server configure

S.No	Command Name	Description	Type and Description
1	save	Save InterlAmt server configuration changes.	
2	cancel	Roll back IntelAmt server configuration changes.	
3	exit	Save IntelAmt server configuration changes and exit current mode.	
4	enable_Intel_Amt	enable/disable Intel Amt Ports.	Boolean choice
5	Wan_hosts	IntelAmt Wan Host Type.	Intel Amt Wan Host type
6	Wan_host_Address	IntelAmt Wan Host Address	String
7	Internal_Address	IntelAmt intenal Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.25 net intel\_Amt\_Reflector configure

S.No	Command Name	Description	Type and Description
1	save	Save InterlAmt Reflector configuration changes.	
2	cancel	Roll back IntelAmt server configuration changes.	
3	exit	Save IntelAmt server configuration changes and exit current mode.	
4	enable	enable intelAmt reflectors on port	
5	enable Intel_Amt_Reflector	enable/disable Ports.	Boolean choice
6	enable Intel_Amt_Reflector_d estport	enable intelamt reflectors on different ports	

S.No	Command Name	Description	Type and Description
7	enable Intel_Amt_Reflectord estport 16992	enable/disable Ports.	Boolean choice
8	enable Intel_Amt_Reflectord estport 16993	enable/disable Ports.	Boolean choice
9	enable Intel_Amt_Reflectord estport 16994	enable/disable Ports.	Boolean choice
10	enable Intel_Amt_Reflectord estport 16995	enable/disable Ports.	Boolean choice
11	enable Intel_Amt_Reflectord estport 9971	enable/disable Ports.	Boolean choice
12	Intel_Amt_Reflectors rcport	set port number for different ports	
13	Intel_Amt_Reflectors rcport 16992	Enter source port value for 16992	Port number
14	Intel_Amt_Reflectors rcport 16993	Enter source port value for 16993	Port number
15	Intel_Amt_Reflectors rcport 16994	Enter source port value for 16994	Port number
16	Intel_Amt_Reflectors rcport 16995	Enter source port value for 16995	Port number
17	Intel_Amt_Reflectors rcport 9971	Enter source port value for 9971	Port number

## 11.26 net ip\_Aliasing server add

S.No	Command Name	Description	Type and Description
1	save	Save Ip Alias server configuration changes.	
2	cancel	Roll back Ip Alias server configuration changes.	
3	exit	Save Ip Alias server configuration changes and exit current mode.	
4	Interface	Select the Interface for the Ip Aliasing	WAN interface type
5	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
6	Subnet_Mask	Subnet mask for ip Aliasing	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

### 11.27 net ip\_Aliasing server edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Editing Ip Aliasing server configuration.	Unsigned integer
2	save	Save Ip Alias server configuration changes.	
3	cancel	Roll back Ip Alias server configuration changes.	
4	exit	Save Ip Alias server configuration changes and exit current mode.	
5	Interface	Select the Interface for the Ip Aliasing	WAN interface type
6	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	Subnet_Mask	Subnet mask for ip Aliasing	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

### 11.28 net ip\_Aliasing server delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Delete Ip Aliasing configuratio	Unsigned integer
2	save	Save Ip Alias server configuration changes.	
3	cancel	Roll back Ip Alias server configuration changes.	
4	exit	Save Ip Alias server configuration changes and exit current mode.	
5	Interface	Select the Interface for the Ip Aliasing	WAN interface type
6	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	Subnet_Mask	Subnet mask for ip Aliasing	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.29 net mode configure

S.No	Command Name	Description	Type and Description
1	save	Save IP Mode configuration changes.	
2	exit	Save IP Mode configuration changes and exit current mode.	
3	cancel	Roll back IP Mode configuration changes.	
4	ip_type	Select IPv4 only or IPv4/IPv6 mode.	Select the ip address type.

## 11.30 net ipv6\_tunnel isatap add

S.No	Command Name	Description	Type and Description
1	save	Save isatap tunnel configuration changes.	
2	exit	Save isatap tunnel configuration changes and exit current mode.	
3	cancel	Roll back isatap tunnel configuration changes.	
4	subnet_prefix	This is the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet.	String
5	end_point_type	This is the endpoint address for the tunnel that starts with this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 network), or a specific LAN IPv4 address	select the local end point address type
6	ipv4_address	The local end point address if not the LAN IPv4 address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.31 net ipv6\_tunnel isatap edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	isatap Tunnel configuration mode.	Unsigned integer
2	save	Save isatap tunnel configuration changes.	

S.No	Command Name	Description	Type and Description
3	exit	Save isaptap tunnel configuration changes and exit current mode.	
4	cancel	Roll back isatap tunnel configuration changes.	
5	subnet_prefix	This is the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet.	String
6	end_point_type	This is the endpoint address for the tunnel that starts with this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 network), or a specific LAN IPv4 address	select the local end point address type
7	ipv4_address	The local end point address if not the LAN IPv4 address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

### 11.32 net ipv6\_tunnel isatap delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	isatap tunnel configuration mode.	Unsigned integer

### 11.33 net routing mode configure

S.No	Command Name	Description	Type and Description
1	save	Save NAT configuration changes.	
2	exit	Save NAT configuration changes and exit current mode.	
3	cancel	Roll back Basic Security Level configuration changes.	
4	type	Select NAT or Transparent or Classical mode.	routing mode type

## 11.34 net wan wan1 ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv4 wan configuration changes.	
2	cancel	Roll back ipv4 wan configuration changes.	
3	exit	Exit from the current configuration.	
4	isp_connection_type	Select among the options: STATIC, DHCP Client, PPPoE, PPTP, L2TP, Russian PPTP, Russian L2TP, Japanese Multiple PPPoE, Dual Access Pppoe	ISP Types.
5	dhcpc	If ISP Type selected is DHCPC, this field gives you options to configure DHCPC credentials	
6	dhcpc get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using DHCP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
7	dhcpc primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	dhcpc secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	dhcpc mac_type	Select the Mac Address Source	Types of mac address source
10	dhcpc mac_address	Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
11	dhcpc hostname	Enter the hostname	String
12	static	If ISP Type selected is STATIC, this field gives you options to configure STATIC credentials	
13	static ip_address	If your ISP has assigned a fixed (static or permanent) IP	IP address AAA.BBB.CCC.DDD

S.No	Command Name	Description	Type and Description
		address, fill this fields with Static IP address assigned to you. This will identify the router to your ISP.	where each part is in the range 0-255
14	static subnet_mask	IPv4 Subnet Mask. This is usually provided by the ISP or your network administrator.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
15	static gateway_address	IP address of the ISP's gateway. This is usually provided by the ISP or your network administrator.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
16	static primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
17	static secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
18	static mac_type	Select the Mac Address Source	Types of mac address source
19	static mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
20	pppoe	If ISP Type selected is PPPoE, this field gives you options to configure PPPoE credentials	
21	pppoe username	Enter the username to authenticate	String
22	pppoe password	Enter the password to authenticate	String
23	pppoe service	Enter the password to authenticate	String
24	pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
25	pppoe connectivity_type	Enter the connectivity type	ISP Connectivity Types.
26	pppoe idletime	Enter the idle time	idle timeout value type.
27	pppoe get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol.	Boolean choice

S.No	Command Name	Description	Type and Description
		Otherwise Enter No and give valid static dns addresses	
28	pppoe primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
29	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
30	pppoe get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
31	pppoe static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
32	pppoe subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
33	pppoe mac_type	Select the Mac Address Source	Types of mac address source
34	pppoe mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
35	pptp	If ISP Type selected is PPTP, this field gives you options to configure PPTP credentials	
36	pptp username	Enter the username to log in	String
37	pptp password	Enter the password to log in	String
38	pptp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
39	pptp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
40	pptp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice



S.No	Command Name	Description	Type and Description
41	pptp mmpe_encryption	Enter the MMPE Encryption	Boolean choice
42	pptp split_tunnel	select the split_tunnel	Boolean choice
43	pptp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
44	pptp server_address	IP address of the PPTP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
45	pptp connectivity_type	Set ISP Type	ISP Connectivity Types.
46	pptp idle_time	Set ISP Type	idle timeout value type.
47	pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
48	pptp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
49	pptp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
50	pptp mac_type	Select the Mac Address Source	Types of mac address source
51	pptp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
52	russ_pptp	If ISP Type selected is Russian dual access PPTP ,this field gives you options to configure credentials	
53	russ_pptp username	Enter the username to log in	String
54	russ_pptp password	Enter the password to log in	String
55	russ_pptp mmpe_encryption	Enter the MMPE Encryption	Boolean choice
56	russ_pptp split_tunnel	select the split_tunnel	Boolean choice
57	russ_pptp server_address	IP address of the PPTP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
58	russ_pptp connectivity_type	Set ISP Type	ISP Connectivity Types.
59	russ_pptp idle_time	Set ISP Type	idle timeout value type.
60	russ_pptp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
61	russ_pptp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
62	russ_pptp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
63	russ_pptp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice
64	russ_pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
65	russ_pptp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
66	russ_pptp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
67	russ_pptp mac_type	Select the Mac Address Source	Types of mac address source
68	russ_pptp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
69	l2tp	If ISP Type selected is L2TP, this field gives you options to configure L2TP credentials	
70	l2tp username	Enter the username to log in	String
71	l2tp password	Enter the password to log in	String
72	l2tp secret	Enter the secret to log in	String
73	l2tp split_tunnel	select the split_tunnel	Boolean choice

S.No	Command Name	Description	Type and Description
74	l2tp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
75	l2tp server_address	IP address of the L2TP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
76	l2tp connectivity_type	Set ISP Type	ISP Connectivity Types.
77	l2tp idle_time	Set ISP Type	idle timeout value type.
78	l2tp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
79	l2tp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
80	l2tp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice
81	l2tp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using L2TP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
82	l2tp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
83	l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
84	l2tp mac_type	Select the Mac Address Source	Types of mac address source
85	l2tp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
86	russ_l2tp	If ISP Type selected is Russian Dual Access L2TP, this field gives you options to configure Russian L2TP credentials	

S.No	Command Name	Description	Type and Description
87	russ_l2tp username	Enter the username to log in	String
88	russ_l2tp password	Enter the password to log in	String
89	russ_l2tp secret	Enter the secret to log in	String
90	russ_l2tp split_tunnel	select the split_tunnel	Boolean choice
91	russ_l2tp server_address	IP address of the L2TP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
92	russ_l2tp connectivity_type	Set ISP Type	ISP Connectivity Types.
93	russ_l2tp idle_time	Set ISP Type	idle timeout value type.
94	russ_l2tp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
95	russ_l2tp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
96	russ_l2tp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
97	russ_l2tp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice
98	russ_l2tp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using L2TP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
99	russ_l2tp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
100	russ_l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
101	russ_l2tp mac_type	Select the Mac Address Source	Types of mac address source
102	russ_l2tp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF

S.No	Command Name	Description	Type and Description
			where each part is in the range 00-FF
103	japanese_pppoe	If ISP Type selected is japanese multiple pppoe,this field gives you options to configure credentials	
104	japanese_pppoe primary_profile	configure the primary pppoe profile	
105	japanese_pppoe primary_profile username	Enter the username to authenticate	String
106	japanese_pppoe primary_profile password	Enter the password to authenticate	String
107	japanese_pppoe primary_profile service	Enter the password to authenticate	String
108	japanese_pppoe primary_profile authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
109	japanese_pppoe primary_profile connectivity_type	Enter the connectivity type	ISP Connectivity Types.
110	japanese_pppoe primary_profile idletime	Enter the idle time	idle timeout value type.
111	japanese_pppoe primary_profile get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
112	japanese_pppoe primary_profile primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
113	japanese_pppoe primary_profile secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
114	japanese_pppoe primary_profile get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP	Boolean choice

S.No	Command Name	Description	Type and Description
		address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	
115	japanese_pppoe primary_profile static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
116	japanese_pppoe primary_profile subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
117	japanese_pppoe secondary_profile	configure the secondary pppoe profile	
118	japanese_pppoe secondary_profile username	Enter the username to authenticate	String
119	japanese_pppoe secondary_profile password	Enter the password to authenticate	String
120	japanese_pppoe secondary_profile service	Enter the password to authenticate	String
121	japanese_pppoe secondary_profile authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
122	japanese_pppoe secondary_profile connectivity_type	Enter the connectivity type	ISP Connectivity Types.
123	japanese_pppoe secondary_profile idletime	Enter the idle time	idle timeout value type.
124	japanese_pppoe secondary_profile get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
125	japanese_pppoe secondary_profile primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
126	japanese_pppoe secondary_profile secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
127	japanese_pppoe secondary_profile get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
128	japanese_pppoe secondary_profile static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
129	japanese_pppoe secondary_profile subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
130	japanese_pppoe mac_type	Select the Mac Address Source	Types of mac address source
131	japanese_pppoe mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
132	dual_pppoe	If ISP Type selected is Dual PPPoE, this field gives you options to configure Dual Access PPPoE credentials	
133	dual_pppoe username	Enter the username to authenticate	String
134	dual_pppoe password	Enter the password to authenticate	String
135	dual_pppoe service	Enter the service to authenticate	String
136	dual_pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
137	dual_pppoe connectivity_type	Enter the connectivity type	ISP Connectivity Types.
138	dual_pppoe idletime	Enter the idle time	idle timeout value type.
139	dual_pppoe get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static Dns address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice

S.No	Command Name	Description	Type and Description
140	dual_pppoe primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
141	dual_pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
142	dual_pppoe get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
143	dual_pppoe static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
144	dual_pppoe subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
145	dual_pppoe mac_type	Select the Mac Address Source	Types of mac address source
146	dual_pppoe mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
147	dual_pppoe get_ip_from_phy	Enter Yes to get ip on physical interface from dhcp server in the internal isp network. Otherwise Enter No and give valid static IP address, subnet mask and gateway	Boolean choice
148	dual_pppoe static_ip_phy	Valid IP Address of physical interface	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
149	dual_pppoe subnet_mask_phy	Valid subnet mask of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
150	dual_pppoe gateway_phy	Valid gateway of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
151	dual_pppoe get_dns_from_isp_ph	Enter Yes to get dns dynamically from interal ISP if you have not been assigned any static Dns address. The	Boolean choice



S.No	Command Name	Description	Type and Description
		y internal ISP will automatically assign an DNS address to the router using Dhcp network protocol. Otherwise Enter No and give valid static dns addresses	
152	dual_pppoe primary_dns_phy	Valid primary DNS Server IP Address of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
153	dual_pppoe secondary_dns_phy	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
154	enable_vlan_tag	Enable vlan on wan1	Boolean choice
155	vlan_Id	Enter Vlan Id	Unsigned integer

### 11.35 net wan wan2 ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv4 wan configuration changes.	
2	cancel	Roll back ipv4 wan configuration changes.	
3	exit	Exit from the current configuration.	
4	isp_connection_type	Select among the options: STATIC, DHCP Client, PPPoE, PPTP, L2TP, Russian PPTP, Russian L2TP, Japanese Multiple PPPoE, Dual Access Pppoe, ThreeG	WAN2 ISP Types.
5	dhcpc	If ISP Type selected is DHCPC, this field gives you options to configure DHCPC credentials	
6	dhcpc get_dns_from_osp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using DHCP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice

S.No	Command Name	Description	Type and Description
7	dhcpc primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	dhcpc secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	dhcpc mac_type	Select Mac Address source	Types of mac address source
10	dhcpc mac_address	Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
11	dhcpc hostname	Enter the hostname	String
12	static	If ISP Type selected is STATIC, this field gives you options to configure STATIC credentials	
13	static ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	static subnet_mask	IPv4 Subnet Mask. This is usually provided by the ISP or your network administrator.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
15	static gateway_address	IP address of the ISP's gateway. This is usually provided by the ISP or your network administrator.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
16	static primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
17	static secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
18	static mac_type	Select the Mac Address Source	Types of mac address source
19	static mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
20	pppoe	If ISP Type selected is PPPoE, this field gives you options to configure PPPoE credentials	
21	pppoe username	Enter the username to authenticate	String
22	pppoe password	Enter the password to authenticate	String

S.No	Command Name	Description	Type and Description
23	pppoe service	Enter the password to authenticate	String
24	pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
25	pppoe connectivity_type	Enter the connectivity type	ISP Connectivity Types.
26	pppoe idletime	Enter the idle time	idle timeout value type.
27	pppoe get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
28	pppoe primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
29	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
30	pppoe get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
31	pppoe static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
32	pppoe subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
33	pppoe mac_type	Select the Mac Address Source	Types of mac address source MAC address
34	pppoe mac_address	enter Valid MAC address	AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
35	pptp	If ISP Type selected is PPTP, this field gives you options to configure PPTP credentials	
36	pptp username	Enter the username to log in	String

S.No	Command Name	Description	Type and Description
37	pptp password	Enter the password to log in	String
38	pptp mmpe_encryption	Enter the MMPE Encryption	Boolean choice
39	pptp split_tunnel	select the split_tunnel	Boolean choice
40	pptp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
41	pptp server_address	IP address of the PPTP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
42	pptp connectivity_type	Set ISP Type	ISP Connectivity Types.
43	pptp idle_time	Set ISP Type	idle timeout value type.
44	pptp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
45	pptp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
46	pptp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice
47	pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
48	pptp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
49	pptp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
50	pptp mac_type	Select the Mac Address Source	Types of mac address source
51	pptp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

S.No	Command Name	Description	Type and Description
52	russ_pptp	If ISP Type selected is Russian dual access PPTP , this field gives you options to configure credentials	
53	russ_pptp username	Enter the username to log in	String
54	russ_pptp password	Enter the password to log in	String
55	russ_pptp mmpe_encryption	Enter the MMPE Encryption	Boolean choice
56	russ_pptp split_tunnel	select the split_tunnel	Boolean choice
57	russ_pptp server_address	IP address of the PPTP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
58	russ_pptp connectivity_type	Set ISP Type	ISP Connectivity Types.
59	russ_pptp idle_time	Set ISP Type	idle timeout value type.
60	russ_pptp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
61	russ_pptp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
62	russ_pptp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
63	russ_pptp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice
64	russ_pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
65	russ_pptp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
66	russ_pptp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
67	russ_pptp mac_type	Select the Mac Address Source	Types of mac address source
68	russ_pptp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
69	l2tp	If ISP Type selected is L2TP, this field gives you options to configure L2TP credentials	
70	l2tp username	Enter the username to log in	String
71	l2tp password	Enter the password to log in	String
72	l2tp secret	Enter the secret to log in	String
73	l2tp split_tunnel	select the split_tunnel	Boolean choice
74	l2tp gateway	IP address assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
75	l2tp server_address	IP address of the L2TP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
76	l2tp connectivity_type	Set ISP Type	ISP Connectivity Types.
77	l2tp idle_time	Set ISP Type	idle timeout value type.
78	l2tp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
79	l2tp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
80	l2tp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice
81	l2tp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using L2TP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
82	l2tp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
83	l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
84	l2tp mac_type	Select the Mac Address Source	Types of mac address source
85	l2tp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
86	russ_l2tp	If ISP Type selected is Russian DualAccessL2TP, this field gives you options to configure L2TP credentials	
87	russ_l2tp username	Enter the username to log in	String
88	russ_l2tp password	Enter the password to log in	String
89	russ_l2tp secret	Enter the secret to log in	String
90	russ_l2tp split_tunnel	select the split_tunnel	Boolean choice
91	russ_l2tp server_address	IP address of the L2TP server (if applicable)	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
92	russ_l2tp connectivity_type	Set ISP Type	ISP Connectivity Types.
93	russ_l2tp idle_time	Set ISP Type	idle timeout value type.
94	russ_l2tp ip_address	If Address Mode is Static,give static ip	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
95	russ_l2tp subnet_mask	If Address Mode is Static,give subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
96	russ_l2tp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
97	russ_l2tp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address.Otherwise Enter No and give valid static IP address	Boolean choice
98	russ_l2tp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using L2TP network protocol.	Boolean choice

S.No	Command Name	Description	Type and Description
		Otherwise Enter No and give valid static dns addresses	
99	russ_l2tp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
100	russ_l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
101	russ_l2tp mac_type	Select the Mac Address Source	Types of mac address source
102	russ_l2tp mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
103	japanese_pppoe	If ISP Type selected is japanese multiple pppoe, this field gives you options to configure credentials	
104	japanese_pppoe primary_profile	configure the primary pppoe profile	
105	japanese_pppoe primary_profile username	Enter the username to authenticate	String
106	japanese_pppoe primary_profile password	Enter the password to authenticate	String
107	japanese_pppoe primary_profile service	Enter the password to authenticate	String
108	japanese_pppoe primary_profile authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
109	japanese_pppoe primary_profile connectivity_type	Enter the connectivity type	ISP Connectivity Types.
110	japanese_pppoe primary_profile idletime	Enter the idle time	idle timeout value type.
111	japanese_pppoe primary_profile get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol.	Boolean choice



S.No	Command Name	Description	Type and Description
		Otherwise Enter No and give valid static dns addresses	
112	japanese_pppoe primary_profile primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
113	japanese_pppoe primary_profile secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
114	japanese_pppoe primary_profile get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
115	japanese_pppoe primary_profile static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
116	japanese_pppoe primary_profile subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
117	japanese_pppoe secondary_profile	configure the secondary pppoe profile	
118	japanese_pppoe secondary_profile username	Enter the username to authenticate	String
119	japanese_pppoe secondary_profile password	Enter the password to authenticate	String
120	japanese_pppoe secondary_profile service	Enter the password to authenticate	String
121	japanese_pppoe secondary_profile authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
122	japanese_pppoe secondary_profile connectivity_type	Enter the connectivity type	ISP Connectivity Types.
123	japanese_pppoe secondary_profile idletime	Enter the idle time	idle timeout value type.
124	japanese_pppoe secondary_profile get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any	Boolean choice

S.No	Command Name	Description	Type and Description
		static IP address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	
125	japanese_pppoe secondary_profile primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
126	japanese_pppoe secondary_profile secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
127	japanese_pppoe secondary_profile get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
128	japanese_pppoe secondary_profile static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
129	japanese_pppoe secondary_profile subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
130	japanese_pppoe mac_type	Select the Mac Address Source	Types of mac address source
131	japanese_pppoe mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
132	dual_pppoe	If ISP Type selected is Dual PPPoE, this field gives you options to configure Dual Access PPPoE credentials	
133	dual_pppoe username	Enter the username to authenticate	String
134	dual_pppoe password	Enter the password to authenticate	String
135	dual_pppoe service	Enter the service to authenticate	String
136	dual_pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.

S.No	Command Name	Description	Type and Description
137	dual_pppoe connectivity_type	Enter the connectivity type	ISP Connectivity Types.
138	dual_pppoe idletime	Enter the idle time	idle timeout value type.
139	dual_pppoe get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static Dns address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
140	dual_pppoe primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
141	dual_pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
142	dual_pppoe get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
143	dual_pppoe static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
144	dual_pppoe subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
145	dual_pppoe mac_type	Select the Mac Address Source	Types of mac address source
146	dual_pppoe mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
147	dual_pppoe get_ip_from_phy	Enter Yes to get ip on physical interface from dhcp server in the internal isp network. Otherwise Enter No and give valid static IP address, subnet mask and gateway	Boolean choice

S.No	Command Name	Description	Type and Description
148	dual_pppoe static_ip_phy	Valid IP Address of physical interface	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
149	dual_pppoe subnet_mask_phy	Valid subnet mask of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
150	dual_pppoe gateway_phy	Valid gateway of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
151	dual_pppoe get_dns_from_isp_ph	Enter Yes to get dns dynamically from internal ISP if you have not been assigned any static Dns address. The internal ISP will automatically assign a DNS address to the router using Dhcp network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
152	dual_pppoe primary_dns_phy	Valid primary DNS Server IP Address of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
153	dual_pppoe secondary_dns_phy	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
154	threeg	If ISP Type selected is THREEG, this field gives you options to configure THREEG credentials	
155	threeg username	Enter the username to authenticate	String
156	threeg password	Enter the password to authenticate	String
157	threeg dial_number	Enter the dail number to connect	String
158	threeg authMethod	Enter the auth type to connect	THREEG Authentication Types.
159	threeg apn	Enter the apn to connect	String
160	threeg connectivity_type	Set ISP Type	ISP Connectivity Types.
161	threeg idle_time	Set ISP Type	idle timeout value type.
162	threeg get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an DNS	Boolean choice

S.No	Command Name	Description	Type and Description
		address to the router using THREEG network protocol. Otherwise Enter No and give valid static dns addresses	
163	threeg primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
164	threeg secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
165	enable_vlan_tag	Enable vlan on wan2	Boolean choice
166	vlan_Id	Enter Vlan Id	Unsigned integer

### 11.36 net wan rollOverWan threeG configure

S.No	Command Name	Description	Type and Description
1	save	Save rollOverWan threeG configuration changes.	
2	cancel	Roll back rollOverWan threeG configuration changes.	
3	exit	Save rollOverWan threeG configuration changes and current mode.	
4	Username	Enter the username required to log in to the ISP.	String
5	Password	Enter the password required to login to the ISP	String
6	Dial-In_Number	Enter the number to dial to the ISP	String
7	Authentication_Protocol	Select one of None, PAP or CHAP Authentication Protocols to connect to the ISP	THREEG Authentication Types.
8	Reconnect_mode	Select Always On: The connection is always on OR On Demand :The connection will close after time specified in Idle_time field	ISP Connectivity Types.
9	Maximum_Idle_time	The connection is automatically ended if it is idle for a specified number of minutes	Idle timeout value type.
10	Get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you	Boolean choice

S.No	Command Name	Description	Type and Description
		have not been assigned any static IP address. The ISP will automatically assign an DNS address to the router using THREEG network protocol. Otherwise Enter No and give valid static dns addresses	
11	Primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
12	Secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DD where each part is in the range 0-255
13	MTU_type	Enter MTU type	mtu type
14	MTU_Size	Enter MTU size	mtu size
15	APN_Required	Enable/Disable apn.	Boolean choice
16	Apn	Enter the APN(Access Point Name) provided by the ISP	String

### 11.37 net wan mode configure

S.No	Command Name	Description	Type and Description
1	save	Save wan mode configuration changes.	
2	cancel	Roll back ipv4 wan configuration changes.	
3	exit	Save wan mode configuration changes and current mode.	
4	wan_mode_type	Select among the options: SINGLE_WAN, AUTO_ROLLOVER	Types of WAN modes
5	rollover	Wan Mode in Auto Rollover	
6	rollover wan_port	Select the Auto rollover WAN port	WAN interface type
7	rollover failover_method	Select the Fail Over detection method	
8	rollover failover_method type	Select the Fail Over detection method	Types of Failover Detection methods
9	rollover failover_method dns		
10	rollover failover_method dns ipaddr_wan		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
11	rollover failover_method ping		
12	rollover failover_method ping ipaddr_wan		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	rollover failover_method retry_interval		idle timeout value type.
14	rollover failover_method retry_attempts		number in range of 2 to 999
15	singleport		
16	singleport wan_port		WAN interface type

### 11.38 net wan port\_setup configure

S.No	Command Name	Description	Type and Description
1	save	Save WAN port settings.	
2	exit	Save WAN port settings and exit current mode.	
3	cancel	Roll back WAN port settings changes.	
4	respond_ping	Disable or Enable ping on WAN side	Boolean choice
5	wan1	WAN1 port settings	
6	wan1 mtu_type	Enter MTU type	mtu type
7	wan1 mtu_size	Enter MTU size for WAN1	mtu size
8	wan1 port_speed	Enter the type of port speed for WAN1	Port Speed types
9	wan2	WAN2 port settings	
10	wan2 mtu_type	Enter MTU type	mtu type
11	wan2 mtu_size	Enter MTU size for WAN2	mtu size
12	wan2 port_speed	Enter the type of port speed for WAN2	Port Speed types

### 11.39 net wan configurable\_port configure

S.No	Command Name	Description	Type and Description
1	save	Save Configurable WAN settings.	

S.No	Command Name	Description	Type and Description
2	exit	Save configurable WAN settings and exit current mode.	
3	cancel	Roll back Configurable WAN settings changes.	
4	port_name	Select the configurable port type.	WAN interface type

## 11.40 net wan wan1 ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv6 wan1 configuration changes.	
2	cancel	Roll back ipv6 wan configuration changes.	
3	exit	Save ipv6 wan1 configuration changes and current mode.	
4	isp_type	Set ISP Type	ISP Types.
5	dhcpc	Set DHCPC Configurations	
6	dhcpc stateless_mode_enable	Set Stateless Mode	stateless mode configuration.
7	dhcpc prefix_delegation_enable	Enable prefix delegation	Boolean choice
8	static	set ipv6 address	
9	static ip_address	set ipv6 address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
10	static prefix	set prefix length	Unsigned integer
11	static gateway_address	Set ipv6 gateway address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
12	static primary_dns	Set ipv6 primary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
13	static secondary_dns	Set ipv6 secondary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
14	pppoe	pppoe over ipv6 configuration parameters	



S.No	Command Name	Description	Type and Description
15	pppoe username	Enter the username to authenticate	String
16	pppoe password	Enter the password to authenticate	String
17	pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
18	pppoe dhcpv6_opt	Enter the dhcpv6 option for configuring additional parameters.	WAN interface type
19	pppoe primary_dns	Valid primary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
20	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

## 11.41 net wan wan2 ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv6 wan2 configuration changes.	
2	cancel	Roll back ipv6 wan2 configuration changes.	
3	exit	Save ipv6 wan2 configuration changes and current mode.	
4	isp_type	Set ISP Type	ISP Types.
5	dhcpc	Set DHCPC Configurations	
6	dhcpc stateless_mode_enable	Set Stateless Mode	stateless mode configuration.
7	dhcpc prefix_delegation_enable	Enable prefix delegation	Boolean choice
8	static	set ipv6 address	
9	static ip_address	set ipv6 address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
10	static prefix	set prefix length	Unsigned integer
11	static gateway_address	Set ipv6 gateway address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

S.No	Command Name	Description	Type and Description
12	static primary_dns	Set ipv6 primary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
13	static secondary_dns	Set ipv6 secondary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
14	pppoe	pppoe over ipv6 configuration parameters	
15	pppoe username	Enter the username to authenticate	String
16	pppoe password	Enter the password to authenticate	String
17	pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
18	pppoe dhcpv6_opt	Enter the dhcpv6 option for configuring additional parameters.	WAN interface type
19	pppoe primary_dns	Valid primary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
20	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

## 11.42 16.44 net routing protocol\_binding add

S.No	Command Name	Description	Type and Description
1	save	Save Protocol-Binding rules configuration changes.	
2	exit	Save Protocol Binding rules configuration changes and exit current mode.	
3	cancel	Roll back configuration changes.	
4	Service	Available Service	service type
5	Local_Gateway	local gateway type	WAN interface type
6	Source_Network	source network type	firewall rule address type
7	Destination_Network	destination network type	firewall rule address type
8	source_address_start	starting IP of the Source Network	IP address AAA.BBB.CCC.DDD

S.No	Command Name	Description	Type and Description
			where each part is in the range 0-255
9	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	destination_address_end	ending IP of the Destiation user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

### 11.43 net routing protocol\_binding edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	protocol_binding rules configuration mode.	Unsigned integer
2	save	Save Protocol-Binding rules configuration changes.	
3	exit	Save Protocol Binding rules configuration changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	Service	Available Service	service type
6	Local_Gateway	local gateway type	WAN interface type
7	Source_Network	source network type	firewall rule address type
8	Destination_Network	destination network type	firewall rule address type
9	source_address_start	starting IP of the Source Network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	destination_address_end	ending IP of the Destiation user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.44 net routing protocol\_binding enable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	protocol_binding rules configuration mode.	Unsigned integer
2	save	Save Protocol-Binding rules configuration changes.	
3	exit	Save Protocol Binding rules configuration changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	Service	Available Service	service type
6	Local_Gateway	local gateway type	WAN interface type
7	Source_Network	source network type	firewall rule address type
8	Destination_Network	destination network type	firewall rule address type
9	source_address_start	starting IP of the Source Network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	destination_address_end	ending IP of the Destiation user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.45 net routing protocol\_binding disable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	protocol_binding rules configuration mode.	Unsigned integer
2	save	Save Protocol-Binding rules configuration changes.	
3	exit	Save Protocol Binding rules configuration changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	Service	Available Service	service type

S.No	Command Name	Description	Type and Description
6	Local_Gateway	local gateway type	WAN interface type
7	Source_Network	source network type	firewall rule address type
8	Destination_Network	destination network type	firewall rule address type
9	source_address_start	starting IP of the Source Network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	destination_address_end	ending IP of the Destiation user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## 11.46 net routing protocol\_binding delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	protocol_binding rules configuration mode.	Unsigned integer
2	save	Save Protocol-Binding rules configuration changes.	
3	exit	Save Protocol Binding rules configuration changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	Service	Available Service	service type
6	Local_Gateway	local gateway type	WAN interface type
7	Source_Network	source network type	firewall rule address type
8	Destination_Network	destination network type	firewall rule address type
9	source_address_start	starting IP of the Source Network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	destination_address_end	ending IP of the Destiation user	IP address AAA.BBB.CCC.DDD

S.No	Command Name	Description	Type and Description
			where each part is in the range 0-255

## 11.47 net radvd configure

S.No	Command Name	Description	Type and Description
1	save	Save radvd configuration changes.	
2	exit	Save radvd configuration changes and exit current mode.	
3	cancel	Roll back radvd configuration changes.	
4	enable	enable the RADVD process here to allow stateless auto configuration of the IPv6 LAN network	Boolean choice
5	mode	select N to send router advertisements (RA™s) to all interfaces else Y	radvd advertizemen mode type
6	interval	The time in seconds between sending unsolicited multicast RA™s. The default is 30 seconds.	PPPOE idle timeout Type.
7	flags	RA Flags	
8	flags managed_enabl	Chose Managed to use the administered /stateful protocol for e address auto configuration	Boolean choice
9	flags other_enable	the Other flag is selected the host uses administered/stateful protocol of other (i.e. non-address) information auto configuration.	Boolean choice
10	preference	Chose between low/medium/high for the preference associated with this router™s RADVD process	radvd preference type
11	mtu	This is used in RA™s to ensure all nodes on the network use the same MTU value in the cases where the	mtu size

S.No	Command Name	Description	Type and Description
		LAN MTU is not well known. The default is 1500	
12	life_time	The lifetime in seconds of the route. The default is 3600 seconds.	Unsigned integer

## 11.48 net radvd pool add

S.No	Command Name	Description	Type and Description
1	save	Save radvd Pool configuration changes.	
2	exit	Save radvd Pool configuration changes and exit current mode.	
3	cancel	Roll back radvd Pool configuration changes.	
4	prefix_type	Option whether to select the prefix type as 6to4 or Global/Local/ISATAP	ipv6 prefix type
5	sla_id	The SLA ID (Site-Level Aggregation Identifier) in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent	Unsigned integer
6	prefix_address	It specifies the IPv6 network address	String
7	prefix_length	The prefix length variable is a decimal value that indicates the number of contiguous, higher order bits of the address that make up the network portion of the address	Unsigned integer
8	prefix_life_time	The length of time over which the requesting router is allowed to use the prefix	Unsigned integer

## 11.49 net radvd pool edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	radvd Pool configuration mode.	Unsigned integer

S.No	Command Name	Description	Type and Description
2	save	Save radvd Pool configuration changes.	
3	exit	Save radvd Pool configuration changes and exit current mode.	
4	cancel	Roll back radvd Pool configuration changes.	
5	prefix_type	Option whether to select the prefix type as 6to4 or Global/Local/ISATAP	ipv6 prefix type
6	sla_id	The SLA ID (Site-Level Aggregation Identifier) in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent	Unsigned integer
7	prefix_address	It specifies the IPv6 network address	String
8	prefix_length	The prefix length variable is a decimal value that indicates the number of contiguous, higher order bits of the address that make up the network portion of the address	Unsigned integer
9	prefix_life_time	The length of time over which the requesting router is allowed to use the prefix	Unsigned integer

### 11.50 net radvd pool delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	radvd pool configuration mode.	Unsigned integer

### 11.51 net routing dynamic configure

S.No	Command Name	Description	Type and Description
1	save	Save dynamic route changes.	
2	exit	Save dynamic routes changes and exit current mode.	
3	cancel	Roll back rip configuration changes.	



S.No	Command Name	Description	Type and Description
4	direction	rip direction None, In only, Out only, Both.	rip direction
5	version	Rip version	rip version
6	authentication_enable	Enable/Disable Authentication for RIP-2B/2M	Boolean choice
7	first_key	first MD5 key	
8	first_key id_number	First MD5 Key Id	Unsigned integer
9	first_key authentication_id	First MD5 Authentication Key	String
10	first_key valid_from	First MD5 Key Not Valid Before entered date	
11	first_key valid_from month	month in which md5 authentication key validity starts	Month in the format MM(01- 12)
12	first_key valid_from day	day in which md5 authentication key validity starts	Day in the format DD(01-31)
13	first_key valid_from year	year in which md5 authentication key validity starts	Year
14	first_key valid_from hour	hour in which md5 authentication key validity starts	HH(00-23) using 24 hour clock
15	first_key valid_from minute	minute in which md5 authentication key validity starts	minute in the format MM(00-59)
16	first_key valid_from second	second in which md5 authentication key validity starts	Second in the format SS(00-59)
17	first_key valid_to	First MD5 Key is Not Valid After entered date	
18	first_key valid_to month	month in which md5 authentication key validity ends	Month in the format MM(01- 12)
19	first_key valid_to day	day in which md5 authentication key validity ends	Day in the format DD(01- 31)
20	first_key valid_to year	year in which md5 authentication key validity ends	Year
21	first_key valid_to hour	hour in which md5 authentication key validity ends	HH(00-23) using 24 hour clock

S.No	Command Name	Description	Type and Description
22	first_key valid_to minute	minute in which md5 authentication key validity ends	minute in the format MM(00-59)
23	first_key valid_to second	second in which md5 authentication key validity ends	Second in the format SS(00-59)
24	second_key	Second MD5 Key Parameters	
25	second_key id_number	Second MD5 Key Id	Unsigned integer
26	second_key authentication_id	Second MD5 Authentication Key	String
27	second_key valid_from	Second MD5 Key Not Valid Before Entered date	
28	second_key valid_to	Second MD5 Key Not Valid After entered date	
29	second_key valid_from month	month in which md5 authentication key validity starts	Month in the format MM(01- 12)
30	second_key valid_from day	day in which md5 authentication key validity starts	Day in the format DD(01- 31)
31	second_key valid_from year	year in which md5 authentication key validity starts	Year
32	second_key valid_from hour	hour in which md5 authentication key validity starts	HH(00-23) using 24 hour clock
33	second_key valid_from minute	minute in which md5 authentication key validity starts	minute in the format MM(00-59)
34	second_key valid_from second	second in which md5 authentication key validity starts	Second in the format SS(00-59)
35	second_key valid_to month	month in which md5 authentication key validity ends	Month in the format MM(01- 12)
36	second_key valid_to day	day in which md5 authentication key validity ends	Day in the format DD(01- 31)
37	second_key valid_to year	year in which md5 authentication key validity ends	Year
38	second_key valid_to hour	hour in which md5 authentication key validity ends	HH(00-23) using 24 hour clock

S.No	Command Name	Description	Type and Description
39	second_key valid_to minute	minute in which md5 authentication key validity ends	minute in the format MM(00-59)
40	second_key valid_to second	second in which md5 authentication key validity ends	Second in the format SS(00-59)

## 11.52 net routing static ipv4 configure <name>

S.No	Command Name	Description	Type and Description
1	<name>	Add new static routes.	Only AtoZ, atoz and 0to9 characters are allowed
2	save	Save static route changes.	
3	exit	Save static routes changes and exit current mode.	
4	cancel	Roll back route configuration changes.	
5	destination_address	Set the destination IP.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	subnet_mask	Set the subnet for this rule.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	gateway_address	Set the gateway IP.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	avail_interface	Displays the interface list available on the router.	
9	interface	Set the interface for which the rule applies.	String
10	metric	Set the metric for this route.	Unsigned integer
11	private_flag	Defines whether the route can be shared with other gateways when RIP is enabled	Boolean choice
12	active_flag	Defines whether its an active route	Boolean choice

## 11.53 net routing static ipv4 edit <name>

S.No	Command Name	Description	Type and Description
1	<name>	Edit existing static routes.	Only AtoZ, atoz and 0to9 characters are allowed
2	save	Save static route changes.	

S.No	Command Name	Description	Type and Description
3	exit	Save static routes changes and exit current mode.	
4	cancel	Roll back route configuration changes.	
5	destination_address	Set the destination IP.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	subnet_mask	Set the subnet for this rule.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	gateway_address	Set the gateway IP.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	avail_interface	Displays the interface list available on the router.	
9	interface	Set the interface for which the rule applies.	String
10	metric	Set the metric for this route.	Unsigned integer
11	private_flag	Defines whether the route can be shared with other gateways when RIP is enabled	Boolean choice
12	active_flag	Defines whether its an active route	Boolean choice

## 11.54 net routing static ipv6 configure <name>

S.No	Command Name	Description	Type and Description
1	<name>	Add new IPV6 static routes.	Only AtoZ, atoz and 0to9 characters are allowed
2	save	Save IPV6 static route changes.	
3	exit	Save IPV6 static routes changes and exit current mode.	
4	cancel	Roll back IPV6 route configuration changes.	
5	destination_address	Set the IPV6 destination IP.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
6	prefix	Set the prefix length for this rule.	Unsigned integer
7	gateway_address	Set the gateway IPV6.	IP address abcd:abcd:abcd:abcd:abcd:abcd:

S.No	Command Name	Description	Type and Description
			abcd:abcd where each part is in the range [0-9A-Fa-f:]
8	interface	Set the interface for which the rule applies.	select the ipv6 interface type
9	metric	Set the metric for this route.	Unsigned integer
10	active_flag	Defines whether its an active IPV6 route	Boolean choice

## 11.55 net routing static ipv6 edit <name>

S.No	Command Name	Description	Type and Description
1	<name>	Edit existing IPV6 static routes.	Only AtoZ, atoz and 0to9 characters are allowed
2	save	Save IPV6 static route changes.	
3	exit	Save IPV6 static routes changes and exit current mode.	
4	cancel	Roll back IPV6 route configuration changes.	
5	destination_address	Set the IPV6 destination IP.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
6	prefix	Set the prefix length for this rule.	Unsigned integer
7	gateway_address	Set the gateway IPV6.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
8	interface	Set the interface for which the rule applies.	select the ipv6 interface type
9	metric	Set the metric for this route.	Unsigned integer
10	active_flag	Defines whether its an active IPV6 route	Boolean choice

## 11.56 net routing static ipv4 delete <name>

S.No	Command Name	Description	Type and Description
1	<name>	Deletes a specific route.	Only AtoZ, atoz and 0to9 characters are allowed

**11.57 net routing static ipv6 delete <name>**

S.No	Command Name	Description	Type and Description
1	<name>	Deletes a specific IPV6 route.	Only AtoZ, atoz and 0to9 characters are allowed

**11.58 net tahi add-default-route <ip\_address>**

S.No	Command Name	Description	Type and Description
1	<ip_address>	Add ipv6 default route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

**11.59 net tahi add-route <ip\_address> <gw>**

S.No	Command Name	Description	Type and Description
1	<ip_address> <gw>	Add ipv6 route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:] IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

**11.60 net tahi del-route <ip\_address> <gw>**

S.No	Command Name	Description	Type and Description
1	<ip_address> <gw>	Add ipv6 route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:] IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

**11.61 net tahi ipv6-Alias-Add(LAN) <ip6\_address>**

S.No	Command Name	Description	Type and Description
1	<ip6_address>	Add ipv6 address to LAN interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:

			abcd:abcd where each part is in the range [0-9A-Fa-f:]
--	--	--	--

### 11.62 net tahi ipv6-Alias-Del(LAN) <ip6\_address>

S.No	Command Name	Description	Type and Description
1	<ip6_address>	Delete an ipv6 address from LAN interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

### 11.63 net tahi ipv6-Alias-Add(WAN) <ip6\_address>

S.No	Command Name	Description	Type and Description
1	<ip6_address>	Add ipv6 address to WAN interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

### 11.64 net tahi ipv6-Alias-Del(WAN) <ip6\_address>

S.No	Command Name	Description	Type and Description
1	<ip6_address>	Delete an ipv6 address from WAN interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

### 11.65 net tahi reachable-time <time>

S.No	Command Name	Description	Type and Description
1	<time>	Sets the reachable time of neighbour cache entries	number in range of 30 to 150

### 11.66 net tahi ping6 <ip> <size>

S.No	Command Name	Description	Type and Description
1	<ip> <size>	Ping6 on LAN interface with count one.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:] number in range of 1 to 1500

## 11.67 net tahi mping6 <*mip*>

S.No	Command Name	Description	Type and Description
1	< <i>mip</i> >	Multicast ping6 on LAN.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

## 11.68 net tahi bping6 <*bip*> <*psize*>

S.No	Command Name	Description	Type and Description
1	< <i>bip</i> > < <i>psize</i> >	ping6.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:] number in range of 1 to 1500

## 11.69 net tahi pmtu-route-add <*ipAdd*>

S.No	Command Name	Description	Type and Description
1	< <i>ipAdd</i> >	Add ipv6 route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]

## 11.70 net tahi interface-down <*interface*>

S.No	Command Name	Description	Type and Description
1	< <i>interface</i> >	Brings selected interface down.	Interfaces type

## 11.71 net tahi interface-up <*interface*>

S.No	Command Name	Description	Type and Description
1	< <i>interface</i> >	Brings selected interface up.	Interfaces type

## 11.72 net tahi start-RA- custom <*fileName*> <*ipAddr*>

S.No	Command Name	Description	Type and Description
1	< <i>fileName</i> > < <i>ipAddr</i> >	Starts RA with configuration file obtained through tftp.	String IP address AAA.BBB.CCC.DDD



S.No	Command Name	Description	Type and Description
			where each part is in the range 0-255

## 11.73 net tahi RA-Start

S.No	Command Name	Description	Type and Description
1	save	Save RA configuration changes.	
2	exit	start RA and exit current mode.	
3	cancel	Roll back RA configuration changes.	
4	Interface	interface on which RA should be sent	Interfaces type
5	AdvSendAdvert	sets AdvSendAdvert value	Boolean choice
6	MaxRtrAdvInterval	sets MaxRtrAdvInterval value	MaxRtrAdvInterval range
7	MinRtrAdvInterval	sets MinRtrAdvInterval value	MinRtrAdvInterval range
8	AdvCurHopLimit	sets AdvCurHopLimit value	AdvCurHopLimit range
9	AdvManagedFlag	sets AdvManagedFlag value	Boolean choice
10	AdvOtherConfigFlag	sets AdvOtherConfigFlag value	Boolean choice
11	AdvDefaultLifetime	sets AdvDefaultLifetime value	AdvDefaultLifetime range
12	AdvReachableTime	sets AdvReachableTime value	AdvReachableTime range
13	AdvRetransTimer	sets AdvRetransTimer value	AdvRetransTimer range
14	AdvLinkMTU	sets AdvLinkMTU value	AdvLinkMTU range
15	prefix	prefix to be advertised	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abcd where each part is in the range [0-9A-Fa-f:]
16	prefixLength	sets prefix length value	IPv6 Prefix length
17	AdvOnLink	sets AdvOnLink value	Boolean choice
18	AdvAutonomous	sets AdvAutonomous value	Boolean choice
19	AdvValidLifetime	sets AdvValidLifetime value	AdvValidLifetime range
20	AdvPreferredLifetime	sets AdvPreferredLifetime value	AdvPreferredLifetime range

## 11.74 net upnp configure

S.No	Command Name	Description	Type and Description
1	save	Save upnp configuration changes.	

S.No	Command Name	Description	Type and Description
2	cancel	Roll back upnp configuration changes.	
3	exit	Save upnp configuration changes and current mode.	
4	enable	Enable/Disable UPNP	Boolean choice
5	Interface	Select the interface from LAN/VLAN	String
6	advertisement	Set upnp advertisement parameters	
7	advertisement period	Set Advertisement Period (in seconds)	UPnP Advertisement Period Type.
8	advertisement time_to_live	Set Advertisement Time To Live (in seconds)	UPnP Advertisement Time To Live Type.
9	avail_vlan	Display available vlan	

### 11.75 net port-vlan lan\_edit <portnamew>

S.No	Command Name	Description	Type and Description
1	<portnamew>	Vlan port name range 1-4.	port ID
2	save	Save vlan configuration changes.	
3	exit	Save vlan changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	mode	Port Vlan mode.	Captive Portal Profile ID
6	pvid	Port Vlan ID.	vlan id possible values

### 11.76 net port-vlan wlan\_edit <ssidName>

S.No	Command Name	Description	Type and Description
1	<ssidName>	SSID to be edited.Use command 'show net wireless_vlan status 'to display all SSID's Name	String
2	save	Save vlan configuration changes.	
3	exit	Save vlan changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	mode	Port Vlan mode.	Captive Portal Profile ID
6	pvid	Port Vlan ID	vlan id possible values

## 11.77 net vlan-membership lan\_edit <portw>

S.No	Command Name	Description	Type and Description
1	<portw>	net vlan membership for the vlan and Wlan port	port ID
2	save	Save Vlan Membership configuration changes.	
3	cancel	Roll back vlan membership configuration changes.	
4	exit	Save vlan membership configuration changes and exit current mode.	
5	membership	vlan membership.Give comma seperated VLAN ID values.	
6	membership add	vlan membership.Give comma seperated VLAN ID values.	String
7	membership remove	vlan membership.Give comma seperated VLAN ID values.	String

## 11.78 net vlan-membership wlan\_edit <ssidName>

S.No	Command Name	Description	Type and Description
1	<ssidName>	SSID to be edited.Use command 'show net wireless_vlan status 'to display all SSID's Name	String
2	save	Save Vlan Membership configuration changes.	
3	cancel	Roll back vlan membership configuration changes.	
4	exit	Save vlan membership configuration changes and exit current mode.	
5	membership	vlan membership.Give comma seperated VLAN ID values.	
6	membership add	vlan membership.Give comma seperated VLAN ID values.	String

S.No	Command Name	Description	Type and Description
7	membership remove	vlan membership.Give comma seperated VLAN ID values.	String

## 11.79 net multiVlan subnet edit <vlanID>

S.No	Command Name	Description	Type and Description
1	<vlanID>	Multivlan server edit mode	vlan id possible values
2	save	Save Multi Vlan server configuration changes.	
3	cancel	Roll back Multi Vlan server configuration changes.	
4	exit	Save Multivlan server configuration changes and exit current mode.	
5	ip-address	IP of given MultiVlan subnetVlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	subnet- mask	Add subnet mask for Multivlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	dhcp-mode	Select the DHCP Mode.	dhcpv4 modes
8	domain- name	domain name for vlan.	String
9	start-ip	starting ip address of the dhcp mode.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	end-ip	ending ip of the Valn.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	primary- dns	Primary dns for the vlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	secondary- dns	Secondary dns for the vlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	default_gw	Set default gateway.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	lease-time	Lease time for the vlan.	number in range of 1 to 24
15	relay- gateway	relay gateway for the vlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
16	enable- dns-proxy	relay gateway for the vlan.	Boolean choice

## 11.80 net vlan config add <vlan\_id>

S.No	Command Name	Description	Type and Description
1	<vlan_id>	Add a vlan.	vlan id possible values
2	save	Save vlan configuration changes.	
3	exit	Save vlan changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	vlan-name	Name for vlan.	Only AtoZ, atoz and 0to9 characters are allowed
6	inter-vlan-routing	Enable/Disable interVlan Routing.	Boolean choice
7	showCP-profiles	available captive portal profiles	
8	captive-portal-type	Access Type for the SSID to be configure	Captive Portal Type for SSID
9	permanent-user	accessType is Permanent User	
10	permanent-user auth-mode	authentication-server for user	Authentication Type for Captive Portal user
11	permanent-user auth-type	authentication-type for user	Radius Authentication type
12	permanent-user CP-profile	captive portal profile for user	Captive Portal Profile ID
13	permanent-user Redirect- Type	captive portal profile for user	network redirect mode
14	temporary-user	accessType is Temporary User	
15	temporary-user CP-profile	captive portal profile for user	Captive Portal Profile ID
16	temporary-user Redirect- Type	captive portal redirect type for user	network redirect mode

## 11.81 net vlan config edit <vlan\_Id>

S.No	Command Name	Description	Type and Description
1	<vlan_Id>	Edit a configured vlan.	vlan id possible values
2	save	Save vlan configuration changes.	
3	exit	Save vlan changes and exit current mode.	
4	cancel	Roll back configuration changes.	

S.No	Command Name	Description	Type and Description
5	vlan-name	Name for vlan.	Only AtoZ, atoz and 0to9 characters are allowed
6	inter-vlan-routing	Enable/Disable interVlan Routing .	Boolean choice
7	showCP-profiles	available captive portal profiles	
8	captive-portal-type	Access Type for the SSID to be configure	Captive Portal Type for SSID
9	permanent-user	accessType is Permanent User	
10	permanent-user auth-mode	authentication-server for user	Authentication Type for Captive Portal user
11	permanent-user auth-type	authentication-type for user	Radius Authentication type
12	permanent-user CP-profile	captive portal profile for user	Captive Portal Profile ID
13	permanent-user Redirect- Type	captive portal profile for user	network redirect mode
14	temporary-user	accessType is Temporary User	
15	temporary-user CP-profile	captive portal profile for user	Captive Portal Profile ID
16	temporary-user Redirect- Type	captive portal redirect type for user	network redirect mode

## 11.82 net vlan config delete <VlanId>

S.No	Command Name	Description	Type and Description
1	<VlanId>	Delete a vlan.	Vlan id possible values.

## 11.83 net dmz configure

S.No	Command Name	Description	Type and Description
1	save	Save van configuration mode.	
2	cancel	Roll Back dmz configuration changes.	
3	exit	Save dmz configuration changes and current mode.	
4	enable_dmz	Enable/Disable DMZ.	enable/disable dmz
5	ip_address	Static IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
6	subnet_mask	Subnet Mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	dhcp_mode	Set DHCP mode.	dhcpv4 modes
8	starting_ip_address	DHCP Starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	ending_ip_address	DHCP ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	primary_dns_server	Primary DNS address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	secondary_dns_server	Secondary DNS server address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	default_gw	Setup default gateway.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	wins_server	Set DHCP WINS server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	lease_time	Set DHCP lease time.	Unsigned integer
15	relay_gateway	Set DHCP Relay gateway server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
16	dns_proxy_enable	Set DNS proxy Enable/Disable.	Boolean choice
17	enable_ldap	Enable/Disable LDAP Server Info.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

## Chapter 12. Configuration commands under branch SECURITY

### 12.1 security advanced\_network attack\_checks configure

S.No	Command Name	Description	Type and Description
1	save	Save Security Checks configuration changes.	
2	exit	Save Security Checks configuration changes and exit current mode.	
3	cancel	Roll back Security Checks configuration changes.	
4	enable_stealth_mode	Enable or Disable Stealth Mode.	Boolean choice
5	block_tcp_flood	Enable or Disable TCP Flood on WAN port.	Boolean choice
6	block_udp_flood	Enable or Disable UDP Flood on LAN port.	Boolean choice
7	allow_lan_icmp	Enable or Disable ICMP Notification on LAN port.	Boolean choice
8	block_spoofed_packets	Allow/Block spoofed packets.	Boolean choice
9	Tcp_Filter_Check	Allow/Block Tcp Filter Check.	Boolean choice
10	block_icmp_notification	Enable or Disable ICMP notifications on Internet Ports.	Boolean choice
11	block_fragmented_packets	Enable or Disable Fragmented Packets on Internet Ports.	Boolean choice
12	block_multicast_packets	Enable or Disable Multicast packets on Internet Ports.	Boolean choice
13	synflood_dectect_rate	Configure the Syn flood Detect Rate	range of packets sent per second in dos attack types.
14	block_spoofed_tcp_rst	Enable or Disable blocking of spoofed tcp RST packets.	Boolean choice
15	block_ftp_bounce_attack	Enable or Disable blocking of FTP Bounce Attack packets.	Boolean choice
16	echostorm_flood_rate	Configure the Echo Storm Flood Rate	range of packets sent per second in dos attack types.
17	icmp_flood_rate	Configure the ICMP flood Rate	range of packets sent per second in dos attack types.



S.No	Command Name	Description	Type and Description
18	udp_connection_limit	Configure max number of simultaneous udp connections to allow	number in range of 25 to 600

## 12.2 security advanced\_network ips setup

S.No	Command Name	Description	Type and Description
1	save	Save ips configuration changes.	
2	exit	Save ips configuration changes and exit current mode.	
3	cancel	Roll back ips configuration changes.	
4	enable_intrusion_prevention	Enable or Disable Intrusion Prevention.	Boolean choice
5	enable_intrusion_detection	Enable or Disable Intrusion Detection.	Boolean choice
6	ips_check_active	Enable or Disable IPS checks.	
7	ips_check_active lan-wan	Enable or Disable ips checks active between LAN and WAN.	Boolean choice
8	ips_check_active dmz-wan	Enable or Disable ips checks active between DMZ and WAN	Boolean choice

## 12.3 security application\_rules add

S.No	Command Name	Description	Type and Description
1	save	Save application rules configuration changes.	
2	exit	Save application rules rules configuration changes and exit current mode.	
3	cancel	Roll back application rules configuration changes.	
4	name	Name of the rule	String
5	enable_rule	specify whether to enable or disable the rule	Boolean choice
6	protocol	Specify whether the port uses the TCP or UDP protocol	type of protocol to be selected for a application rules.
7	interface	Specify whether the port uses the TCP or UDP protocol	interface type

S.No	Command Name	Description	Type and Description
8	outgoing_start_port	start port number of the outgoing traffic	Port number
9	outgoing_end_port	end port of the outgoing traffic	Port number
10	incoming_start_port	start port number of the incoming traffic	Port number
11	incoming_end_port	end port number of the incoming traffic	Port number

## 12.4 security application\_rules edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	application rules rules configuration mode.	Unsigned integer
2	save	Save application rules configuration changes.	
3	exit	Save application rules rules configuration changes and exit current mode.	
4	cancel	Roll back application rules configuration changes.	
5	name	Name of the rule	String
6	enable_rule	specify whether to enable or disable the rule	Boolean choice
7	protocol	Specify whether the port uses the TCP or UDP protocol	type of protocol to be selected for a application rules.
8	interface	Specify whether the port uses the TCP or UDP protocol	interface type
9	outgoing_start_port	start port number of the outgoing traffic	Port number
10	outgoing_end_port	end port of the outgoing traffic	Port number
11	incoming_start_port	start port number of the incoming traffic	Port number
12	incoming_end_port	end port number of the incoming traffic	Port number

## 12.5 security application\_rules delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Application rules rules configuration mode.	Unsigned integer

## 12.6 security firewall custom\_service add

S.No	Command Name	Description	Type and Description
1	save	Save custom services configuration changes.	
2	exit	Save custom services configuration changes and exit current mode.	
3	cancel	Roll back custom services configuration changes.	
4	name	Name of the service for which a rule is to be added	String
5	protocol	Protocol	type of protocol to be selected for a custom service.
6	type	Port type can be Port Range/Multiple Ports	type to be selected for a custom service.
7	destination_start_port	Start port number of the Destination user.	Port number
8	destination_finish_port	End port number of the Destination user.	Port number
9	source_start_port	Start port number of the source user.	Port number
10	source_finish_port	End port number of the source user.	Port number
11	icmp_type	port number of the Destination user	number in range of 0-40(icmp) or 1-255(icmpv6)
12	destination_multiple_port	Muliple Ports of the Destination user, Separate Ports by Comma.	comma separated list of Ports ranging from 1-65535.
13	source_multiple_port	Multiple Ports of the source user, Separate Ports by Comma.	comma separated list of Ports ranging from 1-65535.

## 12.7 security firewall custom\_service edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	custom services configuration mode.	Unsigned integer
2	save	Save custom services configuration changes.	
3	exit	Save custom services configuration changes and exit current mode.	
4	cancel	Roll back custom services configuration changes.	

S.No	Command Name	Description	Type and Description
5	name	Name of the service for which a rule is to be added	String
6	protocol	Protocol	type of protocol to be selected for a custom service.
7	type	Port type can be Port Range/Multiple Ports	type to be selected for a custom service.
8	destination_start_port	Start port number of the Destination user.	Port number
9	destination_finish_port	End port number of the Destination user.	Port number
10	source_start_port	Start port number of the source user.	Port number
11	source_finish_port	End port number of the source user.	Port number
12	icmp_type	port number of the Destination user	number in range of 0-40(icmp) or 1-255(icmpv6)
13	destination_multiple_port	Muliple Ports of the Destination user, Separate Ports by Comma.	comma separated list of Ports ranging from 1-65535.
14	source_multiple_port	Multiple Ports of the source user, Separate Ports by Comma.	comma separated list of Ports ranging from 1-65535.

## 12.8 security firewall custom\_service delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	custom services configuration mode	Unsigned integer.

## 12.9 security blocked\_clients add

S.No	Command Name	Description	Type and Description
1	save	Save blocked clients configuration changes.	
2	exit	Save blocked clients configuration changes and exit current mode.	
3	cancel	Roll back blocked clients configuration changes.	
4	mac_address	Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

S.No	Command Name	Description	Type and Description
5	description	Description or Reason for blocking	String

## 12.10 security blocked\_clients edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Blocked Clients configuration mode.	Unsigned integer
2	save	Save blocked clients configuration changes.	
3	exit	Save blocked clients configuration changes and exit current mode.	
4	cancel	Roll back blocked clients configuration changes.	
5	mac_address	Valid MAC address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
6	description	Description or Reason for blocking	String

## 12.11 security blocked\_clients delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Blocked Clients configuration mode.	Unsigned integer

## 12.12 security dynamic\_filter configure

S.No	Command Name	Description	Type and Description
1	save	Save dynamic filter configuration changes.	
2	choose_filter	Choose dynamic filter type.	
3	choose_filter adult	Select adult category as filter type	Boolean choice
4	choose_filter news	Select news category as filter type	Boolean choice
5	choose_filter jobsearch	Select jobsearch category as filter type	Boolean choice
6	choose_filter gambling	Select gambling category as filter type	Boolean choice
7	choose_filter travel/tourism	Select travel/tourism category as filter type	Boolean choice

S.No	Command Name	Description	Type and Description
8	choose_filter shopping	Select shopping category as filter type	Boolean choice
9	choose_filter entertainment	Select entertainment category as filter type	Boolean choice
10	choose_filter chatroomsims	Select chatrooms/im's category as filter type	Boolean choice
11	choose_filter datingsites	Select datingsites category as filter type	Boolean choice
12	choose_filter gamesites	Select gamesites category as filter type	Boolean choice
13	choose_filter investmentsites	Select investment sites category as filter type	Boolean choice
14	choose_filter e-banking	Select e-banking category as filter type	Boolean choice
15	choose_filter crime/terrorism	Select Crime/Terrorism category as filter type	Boolean choice
16	choose_filter personal-benefits- cults	Select personal benefits/cults category as filter type	Boolean choice
17	choose_filter politics	Select polytics category as filter type	Boolean choice
18	choose_filter sports	Select sports category as filter type	Boolean choice
19	choose_filter www-e-mailsites	Select www-e-mail sites category as filter type	Boolean choice
20	choose_filter violence/undesirable	Select violence/undesirable category as filter type	Boolean choice
21	choose_filter malicious	Select malicious category as filter type	Boolean choice
22	choose_filter searchsites	Select search sites category as filter type	Boolean choice
23	choose_filter healthsites	Select health sites category as filter type	Boolean choice
24	choose_filter clubsandsocialities	Select clubs and socialities category as filter type	Boolean choice
25	choose_filter music/video	Select music/video category as filter type	Boolean choice
26	choose_filter businessoriented	Select business oriented category as filter type	Boolean choice
27	choose_filter government- blacklist	Select government blocking list category as filter type	Boolean choice
28	choose_filter educational	Select educational category as filter type	Boolean choice
29	choose_filter advertising	Select advertising category as filter type	Boolean choice

S.No	Command Name	Description	Type and Description
30	choose_filter drugs/alcohol	Select drugs/alcohol category as filter type	Boolean choice
31	choose_filter computing/it	Select computing/it category as filter type	Boolean choice
32	choose_filter swimsuit/lingerie/models	Select Swimsuit/Lingerie/Models category as filter type	Boolean choice
33	choose_filter remote-control- desktop	Select remote control/desktop category as filter type	Boolean choice

## 12.13 security firewall ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save Firewall IPV4 rules configuration changes.	
2	exit	Save Firewall IPV4 rules configuration changes and exit current mode.	
3	cancel	Roll back IPV4 rules configuration changes.	
4	from_zone	Set from Zone security type	firewall rule type
5	from_zone_vlan	Set From Zone VLAN using corresponding VLAN name	String
6	to_zone	Set to Zone security type	firewall rule type
7	to_zone_vlan	Set To Zone VLAN using corresponding VLAN name	String
8	service	.	
9	service service_custom	Name of the custom service for which a rule is to be added custom name should already be added into custom service	String
10	service service_normal	Name of the service for which a rule is to be added	service type
11	action	Action to be taken by the rule	firewall rule action type
12	schedule	Name of schedule for which the rule is applicable	String
13	source_address_type	Type of the source user	firewall rule address type
14	destination_address_type	Type of the destination user	firewall rule address type
15	snat_address_type	Type of the SNAT address	firewall rule snat address type
16	log	Log Always or Never	firewall rule log enable/disable

S.No	Command Name	Description	Type and Description
17	source_address_start	IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
18	source_address_end	IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
19	destination_address_start	IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
20	destination_address_end	IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
21	qos_priority	Firewall type of service	firewall type of service
22	wan_interface	WAN interface for Source NAT settings	String
23	avail_WAN_interfaces	Displays available interfaces	
24	snat_address	IP of the SNAT Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
25	dnat_port	The port number to use for DNAT, required if port forwarding is enabled	Port number
26	port_forwarding_enable	enable/disable port forwarding based on this firewall rule configuration settings	Boolean choice
27	internal_ip_address	Send to Local Server (DNAT IP), Specifies an IP address and port number of a machine on the Local Network which is hosting the server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
28	dnat_ipaddress	External IP address for DNAT settings	String
29	External_IP_Address	Displays available external ip addresses.	



## 12.14 security firewall ipv4 default\_outbound\_policy <default\_outbound\_policy>

S.No	Command Name	Description	Type and Description
1	<default_outbound_policy>	Firewall Settings, Default Outbound Policy configuration mode.	Boolean choice

## 12.15 security firewall ipv4 edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV4 rules configuration mode.	Unsigned integer
2	save	Save Firewall IPV4 rules configuration changes.	
3	exit	Save Firewall IPV4 rules configuration changes and exit current mode.	
4	cancel	Roll back IPV4 rules configuration changes.	
5	from_zone	Set from Zone security type	firewall rule type
6	from_zone_vlan	Set From Zone VLAN using corresponding VLAN name	String
7	to_zone	Set to Zone security type	firewall rule type
8	to_zone_vlan	Set To Zone VLAN using corresponding VLAN name	String
9	service	.	
10	service service_custom	Name of the custom service for which a rule is to be added custom name should already be added into custom service	String
11	service service_normal	Name of the service for which a rule is to be added	service type
12	action	Action to be taken by the rule	firewall rule action type
13	schedule	Name of schedule for which the rule is applicable	String
14	source_address_type	Type of the source user	firewall rule address type
15	destination_address_type	Type of the destination user	firewall rule address type
16	snat_address_type	Type of the SNAT address	firewall rule snat address type
17	log	Log Always or Never	firewall rule log enable/disable
18	source_address_start	IP of the Source user	IP address AAA.BBB.CCC.DDD

S.No	Command Name	Description	Type and Description
			where each part is in the range 0-255
19	source_address_end	IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
20	destination_address_start	IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
21	destination_address_end	IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
22	qos_priority	Firewall type of service	firewall type of service
23	wan_interface	WAN interface for Source NAT settings	String
24	avail_WAN_interfaces	Displays available interfaces	
25	snat_address	IP of the SNAT Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
26	dnat_port	The port number to use for DNAT, required if port forwarding is enabled	Port number
27	port_forwarding_enable	enable/disable port forwarding based on this firewall rule configuration settings	Boolean choice
28	internal_ip_address	Send to Local Server (DNAT IP), Specifies an IP address and port number of a machine on the Local Network which is hosting the server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
29	dnat_ipaddress	External IP address for DNAT settings	String
30	External_IP_Address	Displays available external ip addresses.	

## 12.16 security firewall ipv4 enable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV4 rules configuration mode.	Unsigned integer

## 12.17 security firewall ipv4 disable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV4 Rules configuration mode	Unsigned integer

## 12.18 security firewall ipv4 delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV4 Rules configuration mode	Unsigned integer

## 12.19 security firewall ipv4 move <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV4 Rule reordering mode.	Row id(s) a,b,c where each part is a valid rowid in the range [0-9]
2	save	Save Firewall IPV4 rule reordering changes.	
3	exit	Save Firewall IPV4 rule reordering changes and exit current mode.	
4	cancel	Roll back IPV4 rule reordering changes.	
5	position	New position for the rule	Unsigned integer

## 12.20 security firewall algs

S.No	Command Name	Description	Type and Description
1	save	Save Firewall algs changes.	
2	exit	Save Firewall algs changes and exit current mode.	
3	cancel	Roll Firewall algs changes.	
4	Rtsp	Protocal to be enabled at ALGs	Boolean choice
5	Sip	Protocal to be enabled at ALGs	Boolean choice
6	H323	Protocal to be enabled at ALGs	Boolean choice
7	Tftp	Protocal to be enabled at ALGs	Boolean choice

## 12.21 security firewall ipv6 configure

S.No	Command Name	Description	Type and Description
S.No	Command Name	Description	Type and Description
1	save	Save Firewall IPV6 rules configuration changes.	
2	exit	Save Firewall IPV6 rules configuration changes and exit current mode.	
3	cancel	Roll back IPV6 rules configuration changes.	
4	rule_type	Type of rule to be added	firewall rule type
5	service	.	
6	service service_custom	Name of the custom service for which a rule is to be added custom name should already be added into custom service	String
7	service service_normal	Name of the service for which a rule is to be added	service type
8	action	Action to be taken by the rule	firewall rule action type
9	schedule	Schedule for which the rule is applicable	String
10	source_address_type	Type of the source user	firewall rule address type
11	destination_address_type	Type of the destination user	firewall rule address type
12	log	Log Always or Never	firewall rule log enable/disable
13	source_start_address	IP of the Source user	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abc where each part is in the range [0-9A-Fa- f:]
14	source_end_address	IP of the Source user	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abc where each part is in the range [0-9A-Fa- f:]
15	source_address_prefix	prefix length of the Source user	String
16	destination_start_address	IP of the Destination user	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abc where each part is in the range [0-9A-Fa- f:]
17	destination_end_address	IP of the Destination user	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abc where each part is in the range [0-9A-Fa- f:]

S.No	Command Name	Description	Type and Description
18	destination_address_prefix	Prefix Length of the Destination user	String

## 12.22 security firewall ipv6 edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV6 rules configuration mode.	Unsigned integer
2	save	Save Firewall IPV6 rules configuration changes.	
3	exit	Save Firewall IPV6 rules configuration changes and exit current mode.	
4	cancel	Roll back IPV6 rules configuration changes.	
5	rule_type	Type of rule to be added	firewall rule type
6	service	.	
7	service service_custom	Name of the custom service for which a rule is to be added custom name should already be added into custom service	String
8	service service_normal	Name of the service for which a rule is to be added	service type
9	action	Action to be taken by the rule	firewall rule action type
10	schedule	Schedule for which the rule is applicable	String
11	source_address_type	Type of the source user	firewall rule address type
12	destination_address_type	Type of the destination user	firewall rule address type
13	log	Log Always or Never	firewall rule log enable/disable
14	source_start_address	IP of the Source user	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abc where each part is in the range [0-9A-Fa- f:]
15	source_end_address	IP of the Source user	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abc where each part is in the range [0-9A-Fa- f:]
16	source_address_prefix	prefix length of the Source user	String
17	destination_start_address	IP of the Destination user	IP address abcd:abcd:abcd:abcd:abcd:abcd:

S.No	Command Name	Description	Type and Description
			abcd:abc where each part is in the range [0-9A-Fa- f:]
18	destination_end_address	IP of the Destination user	IP address abcd:abcd:abcd:abcd:abcd:abcd: abcd:abc where each part is in the range [0-9A-Fa- f:]
19	destination_address_prefix	Prefix Length of the Destination user	String

## 12.23 security firewall ipv6 enable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV6 rules configuration mode	Unsigned integer

## 12.24 security firewall ipv6 disable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV6 Rules configuration mode.	Unsigned integer

## 12.25 security firewall ipv6 delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV6 Rules configuration mode	Unsigned integer

## 12.26 security firewall ipv6 move <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Firewall IPV6 Rule reordering mode.	Row id(s) a,b,c where each part is a valid rowid in the range [0-9]
2	save	Save Firewall IPV6 rule reordering changes.	
3	exit	Save Firewall IPV6 rule reordering changes and exit current mode.	
4	cancel	Roll back IPV6 rule reordering changes.	
5	position	New position for the rule	Unsigned integer

## 12.27 security firewall ipv6 default\_outbound\_policy <default\_outbound\_policy>

S.No	Command Name	Description	Type and Description
1	<default_outbound_policy>	Firewall Settings, IPv6 Default Outbound Policy configuration mode.	Boolean choice

## 12.28 security ids configure

S.No	Command Name	Description	Type and Description
1	save	Save IDS configuration changes.	
2	exit	Save IDS configuration changes and exit current mode.	
3	cancel	Roll back IDS configuration changes.	
4	enable	Enable Intrusion detection system	Boolean choice
5	intrusion_log_enable	Enable/Disable intrusion logs	Boolean choice

## 12.29 security session\_settings configure

S.No	Command Name	Description	Type and Description
1	save	Save security session settings configuration changes.	
2	exit	Save session settings configuration changes and exit current mode.	
3	cancel	Roll back session settings configuration changes.	
4	max_unidentified_sessions	Maximum Unidentified Sessions	Unsigned integer
5	max_half_open_sessions	Maximum Half Open Sessions	Unsigned integer
6	tcp_session_timeout	TCP Session Timeout Duration	Unsigned integer
7	udp_session_timeout	UDP Session Timeout Duration	Unsigned integer
8	other_session_timeout	Other Session Timeout Duration	Unsigned integer

S.No	Command Name	Description	Type and Description
9	tcp_session_cleanup_latency	TCP Session Cleanup Latency	Unsigned integer

## 12.30 security schedules add

S.No	Command Name	Description	Type and Description
1	save	Save schedules configuration changes.	
2	exit	Save schedules configuration changes and exit current mode.	
3	cancel	Roll back schedules configuration changes.	
4	name	Name of the schedule for which a rule is to be added	Only AtoZ, atoz and 0to9 characters are allowed
5	days	schedule days	
6	days all	select all days for schedule days	Boolean choice
7	days monday	select all days for schedule days	Boolean choice
8	days tuesday	select all days for schedule days	Boolean choice
9	days wednesday	select all days for schedule days	Boolean choice
10	days thursday	select all days for schedule days	Boolean choice
11	days friday	select all days for schedule days	Boolean choice
12	days saturday	select all days for schedule days	Boolean choice
13	days sunday	select all days for schedule days	Boolean choice
14	time_of_day	scheduled time of day	
15	time_of_day all_enable	type of schedule activation for time of the day	Boolean choice
16	time_of_day start	start time	
17	time_of_day start mins	minutes	minute in the format MM(00-59)
18	time_of_day start hours	hours	schedule time unit type.
19	time_of_day start meridiem	meridiem	Schedule Meridiem Types.
20	time_of_day end	end time	
21	time_of_day end mins	minutes	minute in the format MM(00-59)



S.No	Command Name	Description	Type and Description
22	time_of_day end hours	hours	schedule time unit type.
23	time_of_day end meridiem	meridiem	Schedule Meridiem Types.

### 12.31 security schedules edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Schedules configuration mode.	Unsigned integer
2	save	Save schedules configuration changes.	
3	exit	Save schedules configuration changes and exit current mode.	
4	cancel	Roll back schedules configuration changes.	
5	name	Name of the schedule for which a rule is to be added	Only AtoZ, atoz and 0to9 characters are allowed
6	days	schedule days	
7	days all	select all days for schedule days	Boolean choice
8	days monday	select all days for schedule days	Boolean choice
9	days tuesday	select all days for schedule days	Boolean choice
10	days wednesday	select all days for schedule days	Boolean choice
11	days thursday	select all days for schedule days	Boolean choice
12	days friday	select all days for schedule days	Boolean choice
13	days saturday	select all days for schedule days	Boolean choice
14	days sunday	select all days for schedule days	Boolean choice
15	time_of_day	scheduled time of day	
16	time_of_day all_enable	type of schedule activation for time of the day	Boolean choice
17	time_of_day start	start time	
18	time_of_day start mins	minutes	minute in the format MM(00-59)
19	time_of_day start hours	hours	schedule time unit type.

S.No	Command Name	Description	Type and Description
20	time_of_day start meridiem	meridiem	Schedule Meridiem Types.
21	time_of_day end	end time	
22	time_of_day end mins	minutes	minute in the format MM(00-59)
23	time_of_day end hours	hours	schedule time unit type.
24	time_of_day end meridiem	meridiem	Schedule Meridiem Types.

### 12.32 security schedules delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Schedules configuration mode.	Unsigned integer

### 12.33 security firewall smtpAlg configure

S.No	Command Name	Description	Type and Description
1	save	save SmtplAlg configuration changes.	
2	exit	Save SmtplAlg configuration changes and exit current mode.	
3	cancel	Roll back SmtplAlg configuration changes.	
4	smtp_Alg_Status	Enable/disable SmtplAlg status	Boolean choice
5	port	Set the port you want to use for Smtpl Alg.	Unsigned integer

### 12.34 security firewall smtpAlg approvedMailId add

S.No	Command Name	Description	Type and Description
1	save	save ApprovedMailId configuration changes.	
2	exit	Save ApprovedMailId configuration changes and exit current mode.	
3	cancel	Roll back ApprovedMailId configuration changes.	
4	approved_Mail_Id	Approved Mail_Id	String

## 12.35 security firewall smtpAlg approvedMailId edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to edit an approved MailId.	Unsigned integer
2	save	save ApprovedMailId configuration changes.	
3	exit	Save ApprovedMailId configuration changes and exit current mode.	
4	cancel	Roll back ApprovedMailId configuration changes.	
5	approved_Mail_Id	Approved Mail_Id	String

## 12.36 security firewall smtpAlg approvedMailId delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to delete an approved MailId.	Unsigned integer

## 12.37 security firewall smtpAlg blockedMailId add

S.No	Command Name	Description	Type and Description
1	save	save BlockedMailId configuration changes.	
2	exit	Save BlockedMailId configuration changes and exit current mode.	
3	cancel	Roll back BlockedMailId configuration changes..	
4	blocked_Mail_Id	Blocked Mail_Id	String

## 12.38 security firewall smtpAlg blockedMailId edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to edit a blocked MailId.	Unsigned integer
2	save	save BlockedMailId configuration changes.	

S.No	Command Name	Description	Type and Description
3	exit	Save BlockedMailId configuration changes and exit current mode.	
4	cancel	Roll back BlockedMailId configuration changes.	
5	blocked_Mail_Id	Blocked Mail_Id	String

### 12.39 security firewall smtpAlg blockedMailId delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to delete a blocked MailId.	Unsigned integer

### 12.40 security firewall smtpAlg subjectList add

S.No	Command Name	Description	Type and Description
1	save	save subjectList configuration changes.	
2	exit	Save subjectList configuration changes and exit current mode.	
3	cancel	Roll back subjectList configuration changes.	
4	subject	Subject in the Mail_Id	String
5	mail_Id	Enter the Mail_Id	String
6	action	Action Allow/Block	Boolean choice

### 12.41 security firewall smtpAlg subjectList edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to edit subject with MailId and action.	Unsigned integer
2	save	save subjectList configuration changes.	
3	exit	Save subjectList configuration changes and exit current mode.	

4	cancel	Roll back subjectList configuration changes.	
5	subject	Subject in the Mail_Id.	String
6	mail_Id	Enter the Mail_Id.	String
7	action	Action Allow/Block.	Boolean choice

## 12.42 security firewall smtpAlg subjectList delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	It allows to delete the configuration.	Unsigned integer

## 12.43 security mac\_filter configure

S.No	Command Name	Description	Type and Description
1	save	Save mac filter configuration changes.	
2	exit	Save mac filter configuration changes and exit current mode.	
3	cancel	Roll back mac filter configuration changes.	
4	enable	Enable/Disable the mac filter status.	Boolean choice
5	policy	Sets the mac address policy.	Policy type for mac addresses

## 12.44 security mac\_filter source add

S.No	Command Name	Description	Type and Description
1	save	Save source mac filter configuration changes.	
2	exit	Save source mac filter configuration changes and exit current mode.	
3	cancel	Roll back source mac filter configuration changes.	
4	address	Enter mac address to which the policies will be applied.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

## 12.45 security mac\_filter source edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Source Mac Filter configuration mode.	Unsigned integer
2	save	Save source mac filter configuration changes.	
3	exit	Save source mac filter configuration changes and exit current mode.	
4	cancel	Roll back source mac filter configuration changes..	
5	address	Enter mac address to which policies will be applied.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

## 12.46 security mac\_filter source delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Source Mac Filter configuration mode	Unsigned integer

## 12.47 security ip\_or\_mac\_binding add

S.No	Command Name	Description	Type and Description
1	save	Save ip mac binding configuration changes.	
2	exit	Save ip mac binding configuration changes and exit current mode.	
3	cancel	Roll back ip mac binding configuration changes.	
4	computer_name	Specify a unique name for this rule.	String
5	mac_address	enter mac address to which policies will be applied.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
6	ip_address	enter ip address to which policies will be applied.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	log_dropped_packets	Specify logging option for this rule.	Boolean choice

## 12.48 security ip\_or\_mac\_binding edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Ip/mac binding configuration mode.	Unsigned integer
2	save	Save ip mac binding configuration changes.	
3	exit	Save ip mac binding configuration changes and exit current mode.	
4	cancel	Roll back ip mac binding configuration changes.	
5	computer_name	Specify a unique name for this rule.	String
6	mac_address	enter mac address to which policies will be applied.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
7	ip_address	enter ip address to which policies will be applied.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	log_dropped_packets	Specify logging option for this rule.	Boolean choice

## 12.49 security ip\_or\_mac\_binding delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	ip/mac binding configuration mode	Unsigned integer

## 12.50 security firewall vpn\_passthrough configure

S.No	Command Name	Description	Type and Description
1	save	Save VPN Passthrough configuration changes.	
2	exit	Save VPN Passthrough configuration changes and exit current mode.	
3	cancel	Roll back VPN Passthrough configuration changes.	
4	ipsec_enable	Enable or Disable IPSEC Passthrough.	Boolean choice

S.No	Command Name	Description	Type and Description
5	pptp_enable	Enable or Disable PPTP Passthrough.	Boolean choice
6	l2tp_enable	Enable or Disable L2TP Passthrough.	Boolean choice

## 12.51 security webAccess status <status>

S.No	Command Name	Description	Type and Description
1	<status>	Security webAccess status.	WPS status

## 12.52 security webAccess add

S.No	Command Name	Description	Type and Description
1	save	Security webAccess configuration.	
2	exit	Save webAccess rules configuration changes and exit current mode.	
3	cancel	Roll back webAccess rules configuration changes.	
4	name	name	String
5	accessType	accessType	Access Type for web access filter
6	ipAddr	IpAddr	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	vlanId	VlanId	Number in the range 1-4095

## 12.53 security webAccess edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	security webAccess edit	Unsigned integer
2	save	security webAccess configuration.	
3	exit	Save webAccess rules configuration changes and exit current mode.	
4	cancel	Roll back webAccess rules configuration changes.	
5	name	name	String
6	accessType	accessType	Access Type for web access filter



S.No	Command Name	Description	Type and Description
7	ipAddr	ipAddr	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	vlanId	vlanId	Number in the range 1-4095

## 12.54 security webAccess delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Security webAccess delete	Unsigned integer

## 12.55 security website\_filter content\_filtering configure

S.No	Command Name	Description	Type and Description
1	save	Save contentFiltering configuration changes.	
2	exit	Save content Filtering configuration changes and exit current mode.	
3	cancel	Roll back content filtering configuration changes.	
4	content_filtering	Enable/Disable content Filtering.	Boolean choice
5	proxy_enable	Enable/Disable proxy.	Boolean choice
6	java_enable	Enable/Disable java.	Boolean choice
7	activex_enable	Enable/Disable activex.	Boolean choice
8	cookies_enable	Enable/Disable cookies.	Boolean choice

## 12.56 security website\_filter approved\_urls add

S.No	Command Name	Description	Type and Description
1	save	Save trusted domains configuration changes.	
2	exit	Save trusted domains configuration changes and exit current mode.	
3	cancel	Roll back trusted domains configuration changes.	
4	url	Trusted domain name.	String

## 12.57 security website\_filter approved\_urls edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Trusted domains configuration mode.	Unsigned integer
2	save	Save trusted domains configuration changes.	
3	exit	Save trusted domains configuration changes and exit current mode.	
4	cancel	Roll back trusted domains configuration changes	
5	url	trusted domain name.	String

## 12.58 security website\_filter approved\_urls delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Trusted Domains configuration mode.	Unsigned integer

## 12.59 security website\_filter blocked\_keywords add

S.No	Command Name	Description	Type and Description
1	save	Save blocked keywords configuration changes.	
2	exit	Save blocked keywords configuration changes and exit current mode.	
3	cancel	Roll back blocked keywords configuration changes.	
4	blocked_keyword	Enter keyword to be blocked.	String

## 12.60 security website\_filter blocked\_keywords edit <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	Blocked Keywords configuration mode.	Unsigned integer

S.No	Command Name	Description	Type and Description
2	save	Save blocked keywords configuration changes.	
3	exit	Save blocked keywords configuration changes and exit current mode.	
4	cancel	Roll back blocked keywords configuration changes.	
5	blocked_keyword	enter keyword to be blocked.	String

### 12.61 security website\_filter blocked\_keywords delete <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	blocked Keywords configuration mode	Unsigned integer

### 12.62 security website\_filter blocked\_keywords enable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	blocked Keywords configuration mode	Unsigned integer

### 12.63 security website\_filter blocked\_keywords disable <row\_id>

S.No	Command Name	Description	Type and Description
1	<row_id>	blocked Keywords configuration mode	Unsigned integer