D-Link®
Building Networks for People

Wireless Controller CLI Reference Guide

DWC-1000

Ver. 1.01

Business Wireless Solution

CLI Reference Guide

Wireless Controller

D-Link Corporation

http://www.dlink.com

CLI Reference Guide

DWC-1000
Wireless Controller
Version 1.01

Copyright Notice

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

This document describes the command line interface (CLI) for managing DWC-1000 (WLAN) wireless contorller.

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

- Note that the following features in the DWC-1000 wireless controller 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 DWC-1000 controller for managing these features.

Chapter 2. Accessing the CLI

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

```
*********************************************

 Welcome to the DWC-1000 Command Line Interface

 *********************************************

D-Link DWC-1000>
```

Note: DWC-1000> is the *CLI prompt.*

Chapter 3. Basic commands available on the CLI

3.1 CONTEXT SENSITIVE HELP

[] - Display 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.

3.2 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.

3.3 MOVEMENT KEYS

[CTRL-A] - Move to the start of the line.

[CTRL-E] - Move to the end of the line.

[up] - Move to the previous command line held in history.

[down] - Move to the next command line held in history.

[left] - Move the insertion point left one character.

[right] - Move the insertion point right one character.

3.4 DELETION KEYS

[CTRL-C] - Delete the whole line.

[CTRL-D] - Delete the character to the right on the insertion point.

[CTRL-K] - Delete all the characters to the right of the insertion point.

[Backspace] - Delete the character to the left of the insertion point.

3.5 ESCAPE SEQUENCES

!! - Substitute the last command line.

!N - Substitute the Nth command line (absolute as per 'history' command).

!-N - Substitute the command line entered N lines before (relative).

Chapter 4. Command Hierarchy in CLI

4.1 CLI commands can be divided into 3 categories:

- Global commands
- Show commands
- Configuration commands

4.2 Configration commands are sub-divided into the following:

- WLAN
- System
- Utilities (UTIL)
- QoS
- Networking (net)
- Virtual Private Area Network (VPN)
- Security
- History
- RADUIS
- License Activation

4.3 The wireless controller configuration is sub-divided into following:

- AP Management
- AP profile configuration
- Distributed Tunnel Configuration

- SNMP configration
- Peer Controller configuration
- WIDS configuration
- AP Validation Configuration
- Country Configuration
- Wireless switch configuration

Chapter 5. Global commands used in CLI

.exit: Exit this session

.help: Display an overview of the CLI syntax

.top: Return to the default mode

.reboot: Reboot the system.

.history: Display 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 6. Show commands used in CLI

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

6.1 WLAN Management

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

Sl No	Command Name	Purpose
1	show wlan ap_management	Display the parameters related to ap management
2	show wlan ap_management channel_plan	Display the configured channel plan parameters.
3	show wlan ap_management power_plan	Display the configured power plan parameters.
4	show wlan ap_management oui	Local OUI Database Entries
5	show wlan ap_management discovery	Display AP and peer switch discovery parameters.
6	show wlan ap_management channel_plan status *<ltradio>*	Display the configured channel plan parameters.
7	show wlan ap_management channel_plan history *<ltradio>*	Display the channel plan history.
8	show wlan ap_management channel_plan proposed *<ltradio>*	Display the proposed channel adjustments.
9	show wlan ap_management power_plan status	Display the configured power plan parameters.
10	show wlan ap_management power_plan proposed	Display the proposed power adjustments.
11	show wlan ap_management oui database	Display Local OUI Database
12	show wlan ap_management discovery status	Display Discovery parameters
13	show wlan ap_management discovery ip_list	Display IP Poll discovery list.
14	show wlan ap_management discovery vlan_list	Display VLAN ID discovery list.
15	show wlan ap_management oui status *<ltouival>*	Display Local OUI Database for a ouival
16	show wlan ap_conf	Display AP configuration and status
17	show wlan ap_conf capability	Display AP hardware capability.
18	show wlan ap_conf macaddr	Display AP configuration and status for specific AP
19	show wlan ap_conf database	Display AP configuration and status.
20	show wlan network	Display network configuration parameters.
21	show wlan ap_conf download	Display AP code download configuration and status.
22	show wlan network status	Display network configuration parameters
23	show wlan network networkid *<ltid>*	Display network configuration parameters for specific network
24	show wlan ap_conf failure_status	Display AP association and authentication failure status.
25	show wlan ap_conf image_availability	Display WS stored AP image information.
26	show wlan ap_conf profile	Display AP profile parameters.
27	show wlan ap_conf provisioning_status	Display AP Provisioning parameteres.
28	show wlan ap_conf radio_status	Display Radio configuration.
29	show wlan ap_conf rf-scan_status	Display WS managed APs RF Scan data.
30	show wlan ap_conf status	Display WS managed AP status

		parameters.
31	show wlan ap_conf capability status	Display AP hardware capability.
32	show wlan ap_conf capability image_table	Display AP image capability table
33	show wlan ap_conf capability hardware *<|thw_dwl8600|hw_dwl3600|hw_dwl6600> <|tradio>*	Display AP hardware capability for specific hardware
34	show wlan ap_conf database status	Display AP configuration and status.
35	show wlan ap_conf database macaddr *<|tmacaddr>*	Display AP configuration and status for specific AP
36	show wlan ap_conf profile status	Display AP profile parameters.
37	show wlan ap_conf profile radio	Display AP profile radio parameters.
38	show wlan ap_conf profile radio status *<|tid> <|tradio>*	Display AP profile radio parameters.
39	show wlan ap_conf profile radio auto_eligible *<|tid> <|tradio>*	Display supported and enabled channels for AP profile radio parameters.
40	show wlan ap_conf profile radio mcs_indices *<|tid> <|tradio>*	Display supported MCS indices for the AP profile radio
41	show wlan ap_conf profile radio qos *<|tid> <|tradio>*	Display QoS parameters for the AP profile radio.
42	show wlan ap_conf profile radio rates *<|tid> <|tradio>*	Display advertised and supported rates for AP profile
43	show wlan ap_conf profile radio tspec *<|tid> <|tradio>*	Display TSPEC parameters for the AP profile radio
44	show wlan ap_conf profile radio vap *<|tid> <|tradio>*	Display AP profile VAP parameters.
45	show wlan ap_conf profile profileid *<|tprofileid>*	Display AP profile parameters for specific profile
46	show wlan ap_conf macaddr dist_tunnel_statistics *<|tmacaddr>*	Display L2 Distributed Tunnel statistics for AP.
47	show wlan ap_conf macaddr dist_tunnel_status *<|tmacaddr>*	Display L2 Distributed Tunnel status for AP.
48	show wlan ap_conf macaddr failure_status *<|tmacaddr>*	Display WS managed AP failure status parameters.
49	show wlan ap_conf macaddr provisioning_status *<|tmacaddr>*	Display AP Provisioning status parameters.
50	show wlan ap_conf macaddr radio_status *<|tmacaddr>*	Display WS managed AP radio status parameters.
51	show wlan ap_conf macaddr rf_scan_rogue_classification *<|tmacaddr>*	Display the WIDS AP rogue classification test results.
52	show wlan ap_conf macaddr rf_scan_status *<|tmacaddr>*	Display RF Scan AP status parameters.
53	show wlan ap_conf macaddr rf_scan_triangulation *<|tmacaddr>*	Display signal triangulation status.
54	show wlan ap_conf macaddr statistics *<|tmacaddr>*	Display WS managed AP statistics.
55	show wlan ap_conf macaddr status *<|tmacaddr>*	Display WS managed AP status parameters.
56	show wlan ap_conf macaddr tspec_statistics *<|tmacaddr>*	Display WS managed AP TSPEC statistics.
57	show wlan ap_conf macaddr tspec_status *<|tmacaddr>*	Display WS managed AP TSPEC status.
58	show wlan client	Display AP associated client configuration and status.
59	show wlan known_client	Display the wireless Known Client(s)
60	show wlan client adhoc	Display Ad Hoc network information.
61	show wlan client detected-client	Display detected clients information
62	show wlan client rrm	Display Radio Resource Measurement (RRM) information.
63	show wlan client summary	Display associated client summary parameters.
64	show wlan client adhoc status	Display WS detected clients on an ad-hoc network
65	show wlan client rrm status	Show associated client Radio Resource Measurement status parameters.
66	show wlan client status	Display associated client status

		parameters.
67	show wlan client detected-client preauth-history	Display detected client pre-auth history status
68	show wlan client detected-client roam-history	Display detected client roam history status.
69	show wlan client detected-client status	Display detected client status parameters.
70	show wlan client macaddr	Show associated client MAC address for specific client
71	show wlan client macaddr detected_client	Display associated detected clients information
72	show wlan client macaddr adhoc *<ltmacaddr>*	Display Ad Hoc network information.
73	show wlan client macaddr client-qos	Display associated client QoS information
74	show wlan client macaddr client-qos radius *<ltmacaddr>*	Display associated client QoS RADIUS configuration.
75	show wlan client macaddr client-qos status *<ltmacaddr>*	Display associated client QoS status parameters.
76	show wlan client macaddr detected_client preauth-history *<ltmacaddr>*	Display detected client pre-auth history status.
77	show wlan client macaddr detected_client roam-history *<ltmacaddr>*	Display detected client roam history status
78	show wlan client macaddr detected_client rogue-classification *<ltmacaddr>*	Display the WIDS Client rogue classification test results.
79	show wlan client macaddr detected_client status *<ltmacaddr>*	Display detected client status parameters.
80	show wlan client macaddr detected_client triangulation *<ltmacaddr>*	Display detected client signal triangulation status
81	show wlan client macaddr dist-tunnel *<ltmacaddr>*	Display associated client L2 Distributed Tunnel information.
82	show wlan client macaddr neighbor_ap *<ltmacaddr>*	Display status parameters of neighbor AP seen by client
83	show wlan client macaddr rrm *<ltmacaddr>*	Display Radio Resource Measurement (RRM) information.
84	show wlan client macaddr statistics status *<ltmacaddr>*	Display WS managed AP client statistics.
85	show wlan client macaddr statistics	Display WS managed AP client statistics.
86	show wlan client macaddr statistics association *<ltmacaddr>*	Display client association statistics.
87	show wlan client macaddr statistics session *<ltmacaddr>*	Display session statistics
88	show wlan client macaddr status *<ltmacaddr>*	Display associated client status parameters.
89	show wlan client macaddr tspec_statistics *<ltmacaddr>*	Display WS managed AP client TSPEC statistics.
90	show wlan client macaddr tspec_status *<ltmacaddr>*	Display associated client TSPEC status parameters.
91	show wlan global	Display global Wireless Switch parameters.
92	show wlan global status	Display all global wireless switch status parameters.
93	show wlan global snmp_trap	Display the wireless switch SNMP trap configuration.
94	show wlan global dist_tunnel	Display L2 Distributed Tunnel status.
95	show wlan global tspec	Display global wireless switch TSPEC information.
96	show wlan global tspec global	Display global wireless switch TSPEC information.
97	show wlan global tspec statistics	Display global wireless switch TSPEC information.
98	show wlan global tspec status	Display global wireless switch TSPEC information.
99	show wlan global statistics	Display the current global wireless switch statistics.
100	show wlan global tunnel_mtu	Display the wireless tunnel MTU value.

101	show wlan global radius	Display global wireless radius parameters.
102	show wlan global country_code	Display valid country codes.
103	show wlan global mac_authentication_mode	Display the wireless MAC authentication mode.
104	show wlan global agetime	Display all database entry age times in hours.
105	show wlan peer_switch	Display status for peer wireless switches and configuration push.
106	show wlan peer_switch configuration	Display status for configuration push.
107	show wlan peer_switch peer_controller	Display status for peer wireless switches
108	show wlan peer_switch peer_controller status	Display status for peer wireless switches
109	show wlan peer_switch peer_controller configuration_status	Display configuration for peer switch configuration push groups.
110	show wlan peer_switch peer_controller configure_status	Display status for peer switch configuration push.
111	show wlan peer_switch peer_controller ip	Display status for peer wireless switch for an IP
112	show wlan peer_switch peer_controller ap_status	Display status for peer switch managed APs
113	show wlan peer_switch peer_controller ip status *<ltipaddr>*	Display status for peer switch .
114	show wlan peer_switch peer_controller ip ap_status *<ltipaddr>*	Display status for peer switch managed APs.
115	show wlan peer_switch peer_controller ip configure_status *<ltipaddr>*	Display status for peer switch configuration push.
116	show wlan peer_switch configuration receive_status	Display status for configuration received from a peer switch.
117	show wlan peer_switch configuration request_status	Display status for a peer switch configuration push request.
118	show wlan wids_security	Display the wireless WIDS security settings
119	show wlan wids_security client	Display the WIDS Client security configuration
120	show wlan wids_security ap	Display the WIDS AP security configuration
121	show wlan wids_security de_authentication	Display the AP de-authentication attack status
122	show wlan wids_security rogue_test_descriptions	isplay the WIDS AP rogue classification test descriptions.
123	show wlan multicast	Display the valid multicast transmit rates.
124	show wlan multicast txrate *<ltradio>*	Display the valid multicast transmit rates
125	show wlan rates *<ltradio>*	Display the valid rates.
126	show wlan ssid	Display client network association information.
127	show wlan ssid status *<ltssid>*	Display AP associated client configuration and status.
128	show wlan ssid client_status	Display AP associated client configuration and status.
129	show wlan switch	Display switch status information.
130	show wlan switch ipaddr	Display switch status information for an IP address
131	show wlan switch certificate_request_status	Display the switch certificate request information
132	show wlan switch client_status	Display switch to associated client status parameters.
133	show wlan switch local	Display Local wireless switch status parameters.
134	show wlan switch local client_status	Display AP associated client configuration and status.
135	show wlan switch local statistics	Display wireless switch Statistics

136	show wlan switch local status	Display wireless switch status parameters
137	show wlan switch local tspec_statistics	Display wireless switch TSPEC statistics
138	show wlan switch local tspec_status	Display wireless switch TSPEC status parameters.
139	show wlan switch ipaddr client_status *<ltipaddr>*	Display AP associated client configuration and status.
140	show wlan switch ipaddr statistics *<ltipaddr>*	Display wireless switch Statistics
141	show wlan switch ipaddr status *<ltipaddr>*	Display wireless switch status parameters
142	show wlan switch ipaddr tspec_statistics *<ltipaddr>*	Display wireless switch TSPEC statistics
143	show wlan switch ipaddr tspec_status *<ltipaddr>*	Display wireless switch TSPEC status parameters.
144	show wlan switch provision_status	Display the switch provisioning information.
145	show wlan rrm	Display radio resource measurement (RRM) switch data.
146	show wlan rrm channel_load	Display channel load information.
147	show wlan rrm neighbors	Display neighbor information.
148	show wlan rrm neighbors status	Display neighbor information.
149	show wlan rrm neighbors ap_status *<ltmacaddr>*	Display RRM information for a managed AP.
150	show wlan rrm channel_load current_request	Show the current channel load request, if any.
151	show wlan rrm channel_load history_status	Display channel load report history information.
152	show wlan rrm channel_load history_detail	Display information for every known report.
153	show wlan rrm channel_load request_data	Show data to use for new channel load requests.
154	show wlan device_location	Display all device location parameters.
155	show wlan device_location status	Display all device location parameters.
156	show wlan device_location ap	Display all AP Triangulation Location Table parameteres.
157	show wlan device_location ap macaadr *<ltmacaddr>*	Display all Triangulation Location Table parameteres for an AP
158	show wlan device_location ap triangulation	Display all Triangulation Location Table parameteres.
159	show wlan device_location ap triangulation status_all	Display Triangulation Location status parameters for all device entries in the triangulation table database.
160	show wlan device_location ap triangulation status_located	Display Triangulation Location status parameters for located device entries in the triangulation table database.
161	show wlan device_location building	Display device location building parameters.
162	show wlan device_location building number *<lt1-8>*	Enter a valid Building number.
163	show wlan device_location building status	Display device location building parameters.
164	show wlan device_location building floor_ap_status	Display device location AP parameters.
165	show wlan device_location building floor_status	Display device location building floor parameters
166	show wlan device_location client	Display all Triangulation Location Table parameteres.
167	show wlan device_location client triangulation	Display all Triangulation Location Table parameteres.
168	show wlan device_location client triangulation status_all	Display Triangulation Location status parameters for all device entries in the triangulation table database.
169	show wlan device_location client triangulation status_located	Display Triangulation Location status parameters for located device entries in the triangulation table database.

170	show wlan device_location client macaadr <*ltmacaadr*>	Display all Triangulation Location Table parameteres for specifc MAC Address
171	show wlan device_location floor_status	Display On-demand location search floor status
172	show wlan device_location global_status	Display On-demand location search global status
173	show wlan device_location floor_status building <*ltbuilding*>	Building Number
174	show wlan device_location floor_status building_floor <*ltbuilding*> <*ltfloor*>	Floor number to search for the device
175	show wlan device_location floor_status all	Display On-demand location search floor status

6.2 System

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:

Sl No	Command Name	Purpose
1	show system logging	.
2	show system logging remote	.
3	show system logging remote setup	Display remote logging configuration
4	show system logging facility	.
5	show system logging facility setup <*ltfacility*>	Display logging facility configuration
6	show system logging ipv4	.
7	show system logging ipv4 setup	Display logging configuration
8	show system logging ipv6	.
9	show system logging ipv6 setup	Display ipv6 logs configuration
10	show system remote_management	.
11	show system remote_management setup	Display remote management over https configuration
12	show system snmp <*ltagentIP*>	Display SNMP configuration
13	show system switch_setting	.
14	show system switch_setting power_mode	Display pow er mode configuration
15	show system switch_setting jumbo_frame	Display jumbo frame configuration
16	show system status	Display system status
17	show system time	.
18	show system time setup	Display Timezone and NTP configuration
19	show system traffic_meter	.
20	show system traffic_meter setup	Display traffic meter configuration
21	show system usb	Display USB Configuration
22	show system firmwareVersion	Get's the firmw are Version.

6.3 Net

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:

Sl No	Command Name	Purpose
1	show net ipv6_tunnel status	Display ipv6 tunnels status
2	show net ddns	.
3	show net ddns setup	Show Dynamic DNS Configuration.
4	show net lan dhcp	.

5	show net lan dhcp reserved_ip	.
6	show net lan dhcp reserved_ip setup	Show list of DHCP Reserved Addresses.
7	show net lan dhcp leased_clients	.
8	show net lan dhcp leased_clients list	Show list of Available DHCP Leased Clients.
9	show net Option dhcpc	Display dhcp client Configuration.
10	show net dmz	.
11	show net dmz setup	Show DMZ Configuration.
12	show net dmz dhcp	.
13	show net dmz dhcp reserved_ip	.
14	show net dmz dhcp reserved_ip setup	Show list of DMZ DHCP Reserved Addresses.
15	show net dmz dhcp leased_clients	.
16	show net dmz dhcp leased_clients list	Show list of Available DMZ DHCP Leased Clients.
17	show net ethernet	Show Ethernet interfaces
18	show net lan	.
19	show net lan ipv4	.
20	show net lan ipv4 setup	Show LAN Configuration.
21	show net lan ipv6	.
22	show net lan ipv6 setup	Show LAN Configuration.
23	show net statistics *<ltinterface>*	Show Interface Statistics
24	show net intel_Amt	show IntelAmt server details
25	show net intel_Amt server	show IntelAmt Server Configurations
26	show net intel_Amt Reflector	show IntelAmt Reflector Configuration
27	show net intel_Amt server setup	Display net Intel_Amt server setup.
28	show net intel_Amt Reflector setup	Display net Intel_Amt Reflector setup.
29	show net lp_Alias	show lp Alias server details
30	show net lp_Alias server	show lp Alias configuration details
31	show net lp_Alias server setup	Display net Intel_Amt server setup.
32	show net mode	.
33	show net mode setup	Display IP MODE configuration
34	show net ipv6_tunnel	.
35	show net ipv6_tunnel setup	Display ipv6 tunnels configuration
36	show net routing mode	.
37	show net routing mode setup	Routing Mode betw een OPTION and LAN
38	show net Option Option1	.
39	show net Option Option1 ipv4	.
40	show net Option Option1 ipv4 status	Display ipv4 Option1 Information.
41	show net Option Option1 ipv4 setup	Display Option1 Setup Information.
42	show net Option Option2	.
43	show net Option Option2 ipv4	.
44	show net Option Option2 ipv4 status	Display ipv4 Option2 Information.
45	show net Option Option2 ipv4 setup	Display Optionn2 Setup Information.
46	show net Option	.
47	show net Option mode	Display Option mode Information.
48	show net Option port_setup	Display Option port Information.
49	show net Option configurable_port	Display configurable port Information.
50	show net Option Option1 ipv6	.
51	show net option Option1 ipv6 status	Display ipv6 Option1 Information.
52	show net Option Option1 ipv6 setup	Display Option1 Setup Information.
53	show net Option Option2 ipv6	.
54	show net Option Option2 ipv6 status	Display ipv6 Option2 Information.
55	show net Option Option2 ipv6 setup	Display Option2 Setup Information.
56	show net routing ospfv2	show OSPFv2 Configuration

57	show net routing ospfv3	show OSPFv3 Configuration
58	show net routing ospfv2 setup	Display OSPFv2 Configuration
59	show net routing ospfv3 setup	Display OSPFv3 Configuration
60	show net port	.
61	show net port management	.
62	show net port management setup	Display port management configuration
63	show net Option pppoe	Display pppoe client Configuration.
64	show net routing protocol_binding	show protocol_binding rules
65	show net routing protocol_binding setup	Display protocol Binding Rules
66	show net radvd	.
67	show net radvd setup	Display RADVD configuration
68	show net routing dynamic	Show dynamic routing setup
69	show net routing dynamic setup	Show dynamic routing Setup.
70	show net routing	Displays routing setup
71	show net routing static	.
72	show net routing static ipv4	.
73	show net routing static ipv4 setup	Show all the configured IPV4 routes.
74	show net routing static ipv6	.
75	show net routing static ipv6 setup	Show all the configured IPV6 routes.
76	show net upnp	Display UPnP Information
77	show net upnp portmap	Display UPnP portmap Information.
78	show net upnp setup	Display UPnP portmap Information.

6.4 VPN

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:

Sl No	Command Name	Purpose
1	show vpn l2tp	show l2tp server details
2	show vpn l2tp server	show l2tp server details
3	show vpn l2tp server setup	Display l2tp server setup.
4	show vpn l2tp server connections	Display l2tp server stats.
5	show vpn pptp client	show pptp client details
6	show vpn pptp client setup	Display pptp client setup.
7	show vpn pptp client_status	show pptp client status details
8	show vpn pptp client_status setup	Display pptp client status setup.
9	show vpn pptp	show pptp server details
10	show vpn pptp server	show pptp server details
11	show vpn pptp server setup	Display pptp server setup.
12	show vpn pptp server connections	Display pptp server stats.
13	show vpn sslvpn	show sslvpn settings
14	show vpn sslvpn client	show sslvpn client settings
15	show vpn sslvpn route	show route settings
16	show vpn sslvpn policy	show sslvpn policy settings
17	show vpn sslvpn portal-layouts	show sslvpn portal-layouts settings
18	show vpn sslvpn portforwarding	show sslvpn portforwarding settings
19	show vpn sslvpn portforwarding appconfig	show sslvpn portforwarding appconfig settings
20	show vpn sslvpn portforwarding hostconfig	show sslvpn portforwarding hostconfig settings
21	show vpn sslvpn resource	show sslvpn resource settings
22	show vpn sslvpn resource-object *<ltresource_name>*	show sslvpn resource object settings

23	show vpn sslvpn users	show sslvpn users mode
24	show vpn sslvpn users domains	show sslvpn domains
25	show vpn sslvpn users groups	show sslvpn groups
26	show vpn sslvpn users users	show sslvpn users
27	show vpn sslvpn users browser_policies *<ltrow_id>*	show sslvpn users policies by browser
28	show vpn sslvpn users login_policies *<ltrow_id>*	show sslvpn users login policies
29	show vpn sslvpn users ip_policies *<ltrow_id>*	show sslvpn users ip policy
30	show vpn ipsec	show vpn policy
31	show vpn ipsec policy	show vpn policy
32	show vpn ipsec policy setup	show vpn policy
33	show vpn ipsec policy status	show vpn status
34	show vpn ipsec dhcp	show vpn ipsec dhcp setup
35	show vpn ipsec dhcp setup	show vpn ipsec dhcp setup

6.5 Security

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:

Sl No	Command Name	Purpose
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 igmp	Display igmp 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 firewall	Display Firew all Rules
10	show security firewall ipv4	Display Firew all Rules
11	show security firewall ipv4 setup	Display Firew all Rules
12	show security firewall algs	Display ALGs protocals status
13	show security firewall ipv6	Display IPV6 Firew all Rules
14	show security firewall ipv6 setup	Display Firew all Rules
15	show security ids	.
16	show security ids setup	Display IDS configuration
17	show security session_settings	Display Session Settings configuration
18	show security schedules	.
19	show security schedules setup	Display Schedules configuration
20	show security mac_filter	.
21	show security mac_filter setup	Display Source Mac Filter configuration
22	show security ip_or_mac_binding	.
23	show security ip_or_mac_binding setup	Display IP/MAC Binding configuration
24	show security firewall vpn_passthrough	.
25	show security firewall vpn_passthrough setup	Display VPN passthrough Configuration
26	show security website_filter	.
27	show security website_filter content_filtering	Display content filtering configuration
28	show security website_filter approved_urls	Display trusted domains configuration
29	show security website_filter blocked_keywords	Display blocked keyw ords configuration

6.6 RADIUS

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

Sl No	Command Name	Purpose
1	radius configure <*ltradius_server*>	RADIUS configuration mode.
2	radius delete <*ltradius_server*>	Delete a RADIUS configuration mode.

6.7 Help

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

Sl No	Command Name	Purpose
1	.help	Display an overview of the CLI syntax

Chapter 7. Configuration commands

7.1 License Activation commands

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

Sl No	Command Name	Purpose
1	license list	List license on the device
2	license activate *<ltactivationKey>*	activate a license on the device.

7.2 Global configuration commands

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

Sl No	Command Name	Purpose
1	.top	Return to the default mode

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

Sl No	Command Name	Purpose
1	.reboot	Reboot the system.

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

Sl No	Command Name	Purpose
1	.exit	Exit this session

7.3 System configuration commands

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

Sl No	Command Name	Purpose
1	system logging	.
2	system logging ipv4	System logging configuration.
3	system logging facility	System log Facility configuration.
4	system logging remote	System remoteLogging configuration.
5	system logging ipv6	System ipv6 logs configuration.
6	system logging ipv4 configure	System logging configuration mode.
7	system logging facility configure *<ltfacility>*	System logging facility configuration mode.

8	system logging remote configure	System remote Logging configuration mode.
9	system logging ipv6 configure	System ipv6 logs configuration mode.
10	system remote_management	Remote Mgmt Setup.
11	system remote_management https	Remote Mgmt Setup for https.
12	system remote_management https configure	Configure remote management support for https.
13	system remote_management telnet configure	Configure remote management support for telnet.
14	system snmp	System SNMP configuration.
15	system snmp trap	System SNMP trap configuration.
16	system snmp sys	System SNMP system configuration.
17	system snmp access	System SNMP Access Configuration.
18	system snmp users	System SNMP v3 User Configuration.
19	system snmp trap configure *<ltagent_ip>*	SNMP trap configuration mode.
20	system snmp trap delete *<ltagent_ip>*	Delete a SNMP trap configuration.
21	system snmp users configure *<ltuser>*	SNMP v3 User list configuration changes
22	system snmp sys configure	SNMP system configuration mode
23	system snmp access add	snmp access configuration mode
24	system snmp access edit *<ltrowid>*	snmp configuration mode
25	system snmp access delete *<ltrowid>*	snmp access configuration mode
26	system switch_settings	switch setting setup.
27	system switch_settings power_saving	power saving setup.
28	system switch_settings jumbo_frame	jumbo frame setup.
29	system switch_settings power_saving configure	power saving configuration mode.
30	system switch_settings jumbo_frame configure	jumbo frame configuration mode.
31	system time	System time configuration mode
32	system time configure	System time configuration mode
33	system traffic_meter	traffic meter Configuration setup.
34	system traffic_meter configure	traffic meter configuration mode.
35	system usb	USB Configuration.
36	system usb usb1	USB1 Configuration.
37	system usb usb1 configure	USB1 Configuration.
38	system usb usb2	USB2 Configuration.
39	system usb usb2 configure	USB2 Configuration.
40	system users	System user configuration commands.
41	system group	System group configuration commands.
42	system groups configure	System groups configuration mode.
43	system group add	system groups add mode.
44	system group edit *<ltrow_id>*	system groups edit mode.
45	system group delete *<ltrow_id>*	system groups delete mode.
46	system group show *<ltrow_id>*	system groups display mode.
47	system users add	system users add mode.
48	system users edit *<ltrow_id>*	system users edit mode.
49	system users delete *<ltrow_id>*	system users delete mode.
50	system users show *<ltrow_id>*	system users display mode.
51	system users password *<ltuser>*	Change password.
52	system users idle_timeout *<lttimeout>*	Change idle timeout.
53	system group groupaccesscontrol	group access control
54	system group groupaccesscontrol configure *<ltgroup_id>*	group access control configuration
55	system group groupaccesscontrol show *<ltgroup_id>*	Displays Group Access Control

		configuration for the selected group
56	system group access_control_browser	List of browsers for which login policies can be applied
57	system group access_control_browser add	Add a browser to Access Control browsers list
58	system group access_control_browser delete *<ltrow_id>*	Delete a browser from Access Control browsers list
59	system group access_control_browser show	Displays Access Control browsers list
60	system group access_control_ip	List of ips for which login policies can be applied
61	system group access_control_ip add	Add an ip to Access Control ips list
62	system group access_control_ip delete *<ltrow_id>*	Delete an ip from Access Control ips list
63	system group access_control_ip show	Displays Access Control ips list

7.4 UTIL configuration commands

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

Sl No	Command Name	Purpose
1	util restore-factory-defaults	Revert to factory default settings.
2	util system_check	system check options
3	util system_check ping *<ltip_address>*	Ping an Internet Address.
4	util system_check dns_lookup *<ltdns>*	To retrieve the IP address of a Web, FTP, Mail or any other Server on the Internet
5	util system_check traceroute *<ltip_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 capturePackets	Allows you to capture all packets that pass through the selected interface
8	util system_check capturePackets start *<ltinterface>*	Start the packet capture
9	util system_check capturePackets stop	Stop the packet capture
10	util system_check capturePackets download *<ltfileName> <ltipAddr>*	Download the packet capture to the host machine
11	util reboot	Reboot the system.
12	util cat *<ltfileName>*	Concatenate files and print on the standard output.
13	util md5sum *<ltfileName>*	Compute and check MD5 message digest.
14	util copy *<ltfileName1> <ltfileName2>*	Copy the Files.
15	util usb_test *<ltipAddr> <ltfileName>*	To test the USB.

7.5 QoS configuration commands

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

Sl No	Command Name	Purpose
1	qos lan	Configure qos parameters for lan
2	qos option	Configure qos parameters for option

3	qos lan trustmode	trustmode configuration in the sw itch
4	qos lan trustmode cos	Configure cos based QoS on lan
5	qos lan trustmode dscp	Configure dscp based QoS on lan
6	qos lan cos-to-dscp-remarking	enable cos-to-dscp-remarking
7	qos lan queue	queue sheduling and management configuration
8	qos lan cos-map	configures the cos-map for the sw itch port
9	qos lan dscp-map	configures the cos-map for the sw itch port
10	qos lan queue management	lan queue managenet configuation
11	qos lan queue scheduling-algo	lan queue scheduling algorithm configuration
12	qos lan status	Display status of lan QoS
13	qos lan enable	enable QoS on LAN
14	qos lan disable	disable QoS on LAN
15	qos lan trustmode show	show the trustmode on the sw itch
16	qos lan trustmode cos enable *<ltlanPort>*	configures CoS LAN, QoS has to be enabled first.
17	qos lan trustmode dscp enable *<ltlanPort>*	configures DSCP on LAN, QoS has to be enabled first.
18	qos lan cos-map configure *<ltcosValue>* *<ltpriorityQueue>*	configure cos map for qos
19	qos lan cos-map show	show the cos-map for qos
20	qos lan dscp-map show	display dscp priority mappin on sw itch
21	qos lan dscp-map configure *<ltdscpValue>* *<ltpriorityQueue>*	Configure DSCP map for qos
22	qos lan cos-to-dscp-remarking enable	enables cos-to-dscp remarking
23	qos lan cos-to-dscp-remarking disable	disables cos-to-dscp remarking
24	qos lan cos-to-dscp-remarking status	Display status of cos-to-dscp-remarking
25	qos lan cos-to-dscp-remarking configure *<ltcosValue>* *<ltdscpValue>*	configures cos-to-dscp remarking
26	qos option status	Display QoS status on OPTION
27	qos option enable	Enable QoS on option interface
28	qos option disable	Disable QoS on option interface
29	qos option bandw idth set *<ltwanInterface>* *<ltupStreamBW>* *<ltdownStreamBW>*	set the bandw idth for optional option
30	qos option bandw idth	configure bandwidth for option interface
31	qos option traffic-selector	configure traffic selector configuration
32	qos option traffic-selector add	configure traffic selector configuration
33	qos option bandw idth profile	configure bandwidth profiles for option interface
34	qos option bandw idth show *<ltwanInterface>*	Display bandw idth setting for dedicated option
35	qos option bandw idth profile add *<ltwanInterface>* *<ltbwProfileName>* *<ltpriority>* *<ltmaxBW>* *<ltminBW>*	add a bw -profile for option
36	qos option bandw idth profile del *<ltbwProfileName>*	delete a bw -profile on option
37	qos option bandw idth profile show	display all the bandw idth profiles that are configured
38	qos option traffic-selector show	show s the traffic selectors for the option interface
39	qos option traffic-selector add ip *<ltipAddress>* *<ltservice>* *<ltbwProfile>*	add a traffic selector for option
40	qos option traffic-selector add mac *<ltmacAddress>*	add a traffic selector for option

	<ltservice> <ltbwProfile>	
41	qos option traffic-selector add port *<ltlanPort> <ltservice> <ltbwProfile>*	add a traffic selector for option
42	qos option traffic-selector add vlan *<ltvlanId> <ltservice> <ltbwProfile>*	add a traffic selector for option
43	qos option traffic-selector add dscp *<ltdscpId> <ltservice> <ltbwProfile>*	add a traffic selector for option
44	qos option traffic-selector del *<lttrafficSelectorId>*	delete a traffic selector for option
45	qos lan queue management show	queue management configuation show
46	qos lan queue scheduling-algo set *<ltsched-algo>*	set the queue scheduling algorithm in the LAN switch
47	qos lan queue scheduling-algo show	show the queue scheduling algorithm in the LAN switch

7.6 NET configuration commands

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

Sl No	Command Name	Purpose
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 ddns	DDNS setup.
5	net ddns Option1	DDNS setup.
6	net ddns Option2	DDNS setup.
7	net ddns Option1 configure	DDNS configuration mode.
8	net ddns Option2 configure	DDNS configuration mode.
9	net lan dhcp	DHCP setup.
10	net lan dhcp reserved_ip	DHCP Reserved IPs setup.
11	net lan dhcp reserved_ip configure *<ltmac_address>*	DHCP Reserved IPs add/edit mode.
12	net lan dhcp reserved_ip delete *<ltmac_address>*	Delete a specific reserved ip entry.
13	net Option dhcpc	DHCP client configuration mode
14	net Option dhcpc configure	DHCP client configuration mode
15	net dmz	dmz configuration mode
16	net dmz configure	dmz configuration mode
17	net dmz dhcp	DHCP setup.
18	net dmz dhcp reserved_ip	DHCP Reserved IPs setup.
19	net dmz dhcp reserved_ip configure *<ltmac_address>*	DHCP Reserved IPs add/edit mode.
20	net dmz dhcp reserved_ip delete *<ltmac_address>*	Delete a specific reserved ip entry.
21	net ethernet	Ethernet configuration.
22	net ethernet configure *<ltinterface_name>*	Ethernet configuration mode.
23	net lan	LAN setup.
24	net lan ipv4	.
25	net lan ipv4 configure	IPv4 LAN configuration mode.
26	net lan ipv6	.
27	net lan ipv6 configure	IPv6 LAN configuration mode.
28	net lan ipv6 pool	.
29	net lan ipv6 pool configure *<ltipv6PoolStartAddr>*	IPv6 LAN configuration add/edit mode.
30	net lan ipv6 pool delete *<ltipv6PoolStartAddr>*	IPv6 LAN configuration delete.
31	net intel_Amt	net policy mode.

32	net intel_Amt server	net policy mode.
33	net intel_Amt server configure	Intel Amt server configuration mode
34	net intel_Amt_Reflector	net policy mode.
35	net intel_Amt_Reflector configure	Intel Amt Reflector configuration mode
36	net ip_Aliasing	net policy mode.
37	net ip_Aliasing server	net policy mode.
38	net ip_Aliasing server add	Ip Aliasing server configuration
39	net ip_Aliasing server edit *<ltrow_id>*	Editing Ip Aliasing server configuration.
40	net ip_Aliasing server delete *<ltrow_id>*	Delete Ip Aliasing configuratio
41	net mode	IP Mode Setup
42	net mode configure	IP Mode configuration mode.
43	net ipv6_tunnel isatap	isatap tunnel configuration setup.
44	net ipv6_tunnel isatap add	isatap tunnel configuration mode.
45	net ipv6_tunnel isatap edit *<ltrow_id>*	isatap Tunnel configuration mode.
46	net ipv6_tunnel isatap delete *<ltrow_id>*	isatap tunnel configuration mode.
47	net routing mode	Routing Mode betw een OPTION and LAN setup.
48	net routing mode configure	Routing Mode betw een OPTION and LAN configuration mode.
49	net Option Option1	Option1 configuration mode
50	net Option Option1 ipv4	ipv4 Option1 configuration mode
51	net Option Option1 ipv4 configure	ipv4 Option Option1 configuration mode
52	net Option Option2	Option2 configuration mode
53	net Option Option2 ipv4	ipv4 Option2 configuration mode
54	net Option Option2 ipv4 configure	ipv4 Option Option2 configuration mode
55	net Option	Option mode configuration mode
56	net Option mode	Option mode configuration mode
57	net Option mode configure	Option mode configuration mode
58	net Option port_setup	Option port setup.
59	net Option port_setup configure	Option port configuration mode.
60	net Option configurable_port	configurable port setup.
61	net Option configurable_port configure	configurable port setup.
62	net Option Option1 ipv6	ipv6 Option configuration mode
63	net Option Option1 ipv6 configure	ipv6 Option1 configuration mode
64	net Option Option2 ipv6	ipv6 Option2 configuration mode
65	net Optionn Option2 ipv6 configure	ipv6 Option2 configuration mode
66	net routing ospfv2	OSPF Configuration for IPV4
67	net routing ospfv3	OSPF Configuration for IPV6
68	net routing ospfv2 configure *<ltinterface>*	ospfv2 configuration mode.
69	net routing ospfv3 configure *<ltinterface>*	ospfv3 configuration mode.
70	net port	.
71	net port management	port management configuration setup.
72	net port management configure *<ltportName>*	port management configuration mode.
73	net Option pppoe	PPPOE client configuration mode
74	net Option pppoe configure	PPPOE client configuration mode
75	net routing protocol_binding	protocol_binding rules
76	net routing protocol_binding add	protocol_binding rules configuration mode.
77	net routing protocol_binding edit *<ltrow_id>*	protocol_binding rules configuration mode.
78	net routing protocol_binding enable *<ltrow_id>*	protocol_binding rules configuration mode.

79	net routing protocol_binding disable *<ltrow_id>*	protocol_binding rules configuration mode.
80	net routing protocol_binding delete *<ltrow_id>*	protocol_binding rules configuration mode.
81	net radvd	RADVD configuration setup.
82	net radvd pool	RADVD configuration setup.
83	net radvd configure	radvd configuration mode.
84	net radvd pool add	radvd Pool configuration mode.
85	net radvd pool edit *<ltrow_id>*	radvd Pool configuration mode.
86	net radvd pool delete *<ltrow_id>*	radvd pool configuration mode.
87	net routing dynamic	Configure the routes dynamically.
88	net routing dynamic configure	configure the routes dynamically.
89	net routing	configure routing mode, static and dynamic route(s).
90	net routing static	Configure the routes.
91	net routing static ipv4	Configure the routes.
92	net routing static ipv6	Configure the IPV6 routes.
93	net routing static ipv4 configure *<ltname>*	Add new static routes.
94	net routing static ipv6 configure *<ltname>*	Add new IPV6 static routes.
95	net routing static ipv4 delete *<ltname>*	Delete a specific route.
96	net routing static ipv6 delete *<ltname>*	Delete a specific IPV6 route.
97	net routing static ipv4 deleteAll	Delete all the configured routes.
98	net routing static ipv6 deleteAll	Delete all the configured IPV6 routes.
99	net tahi	settings for tahi test suite.
100	net tahi add-default-route *<ltip_address>*	add ipv6 default route on lan interface.
101	net tahi delete-default-route	delete ipv6 default route on lan interface.
102	net tahi add-route *<ltip_address>* *<ltgw>*	add ipv6 route on lan interface.
103	net tahi del-route *<ltip_address>* *<ltgw>*	add ipv6 route on lan interface.
104	net tahi stop-RA	stop sending RA.
105	net tahi start-RA-AdvRetransTimer(1000)	start sending RA with AdvRetransTimer as 1000.
106	net tahi start-RA-AdvRetransTimer(5000)	start sending RA with AdvRetransTimer as 5000.
107	net tahi startRA-Reachable(30000)Retrans(1000)	start sending RA with AdvReachableTime as 30000 and AdvRetransTimer as 1000.
108	net tahi start-RA-AdvReachableTime(10000)	start sending RA with AdvReachableTime as 10000.
109	net tahi start-RA-AdvReachableTime(30000)	start sending RA with AdvReachableTime as 30000.
110	net tahi start-RA(Default)	start sending RA with default parameters.
111	net tahi start-RA-MinValues	start sending RA with minimum values of parameters.
112	net tahi start-RA-MaxValues	start sending RA with maximum values of parameters.
113	net tahi start-RA-MaxRtrAdvInterval(10)	start sending RA with MaxRtrAdvInterval value of 10.
114	net tahi start-RA-MaxRtrAdvInterval(40)	start sending RA with MaxRtrAdvInterval value of 40.
115	net tahi start-RA-MinRtrAdvInterval(198)	start sending RA with MinRtrAdvInterval value of 198.
116	net tahi start-RA-prefix(8000::)	start sending RA with prefix 8000::/64.
117	net tahi start-RA-prefix(fec0::)	start sending RA with prefix fec0::/64.
118	net tahi start-RA-AdvCurHopLimit(0)	start sending RA with AdvCurHopLimit value as 0.

119	net tahi start-RA-AdvCurHopLimit(15)	start sending RA with AdvCurHopLimit value as 15.
120	net tahi ipv6-down	disable the ipv6 stack on the router.
121	net tahi ipv6-up	enable the ipv6 stack on the router.
122	net tahi ipv6-global-up	enable the ipv6 stack on the router and adds global ip.
123	net tahi ipv6-Alias-Add(LAN) *<ltip6_address>*	Add ipv6 address to LAN interface.
124	net tahi ipv6-Alias-Del(LAN) *<ltip6_address>*	Delete an ipv6 address from LAN interface.
125	net tahi ipv6-Alias-Add(OPTION) *<ltip6_address>*	Add ipv6 address to OPTION interface.
126	net tahi ipv6-Alias-Del(OPTION) *<ltip6_address>*	Delete an ipv6 address from OPTION interface.
127	net tahi neigh-cache-del	deletes the ipv6 neighbor cache.
128	net tahi reachable-time *<lttime>*	set the reachable time of neighbour cache entries
129	net tahi mcast-start	start ipv6 multicast
130	net tahi mcast-stop	stop ipv6 multicast
131	net tahi ping6 *<ltip>* *<ltsize>*	ping6 on LAN interface with count one
132	net tahi pmtu-route-add *<ltipAdd>*	add ipv6 route on lan interface.
133	net tahi disable-ipv6-firewall	disable ipv6 firewall.
134	net tahi show-LAN-ip	show ipv6 addresses of LAN interface.
135	net upnp	Upnp configuration mode
136	net upnp configure	Upnp configuration mode

7.7 VPN configuration commands

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

Sl No	Command Name	Purpose
1	vpn l2tp	vpn policy mode.
2	vpn l2tp server	vpn policy mode.
3	vpn l2tp server configure	l2tp server configuration mode
4	vpn pptp client	vpn policy mode.
5	vpn pptp client configure	pptp client configuration mode
6	vpn pptp client_action *<ltaction>*	vpn pptp client action set.
7	vpn pptp	vpn policy mode.
8	vpn pptp server	vpn policy mode.
9	vpn pptp server configure	pptp server configuration mode
10	vpn sslvpn	sslvpn configuration commands
11	vpn sslvpn portal-layouts	sslvpn portal layout configuration commands
12	vpn sslvpn portal-layouts add	Add sslvpn portal layout
13	vpn sslvpn portal-layouts edit *<ltrow_id>*	Edit sslvpn portal layout
14	vpn sslvpn portal-layouts delete *<ltrow_id>*	Delete sslvpn portal layout
15	vpn sslvpn portal-layouts set-default *<ltrow_id>*	Set the portal as default
16	vpn sslvpn portforwarding	sslvpn portforwarding configuration commands
17	vpn sslvpn portforwarding appconfig	sslvpn portforwarding application configuration commands
18	vpn sslvpn portforwarding appconfig add	Add an application configuration rule
19	vpn sslvpn portforwarding appconfig delete *<ltrow_id>*	Delete an application configuration rule
20	vpn sslvpn portforwarding hostconfig	sslvpn portforwarding host

		configuration commands
21	vpn sslvpn portforwarding hostconfig add	Add a host configuration rule
22	vpn sslvpn portforwarding hostconfig delete *<ltrow_id>*	Delete a host configuration rule
23	vpn sslvpn resource	sslvpn resource configuration commands
24	vpn sslvpn resource add	Add an sslvpn resource
25	vpn sslvpn resource configure	Configure an sslvpn resource
26	vpn sslvpn resource configure add *<ltresource_name>*	Add an sslvpn resource object
27	vpn sslvpn resource configure delete *<ltrow_id>*	Delete an sslvpn resource object
28	vpn sslvpn resource delete *<ltrow_id>*	Delete an sslvpn resource
29	vpn sslvpn policy	sslvpn policy configuration commands
30	vpn sslvpn policy add	Add an sslvpn policy
31	vpn sslvpn policy edit *<ltrow_id>*	Edit an sslvpn policy
32	vpn sslvpn policy delete *<ltrow_id>*	Delete an sslvpn policy
33	vpn sslvpn client	sslvpn client configuration commands
34	vpn sslvpn route	sslvpn route configuration commands
35	vpn sslvpn route add	Add sslvpn client route
36	vpn sslvpn route delete *<ltrow_id>*	Delete sslvpn client route
37	vpn sslvpn users	System user configuration commands.
38	vpn sslvpn users domains	System user configuration commands.
39	vpn sslvpn users groups	System user configuration commands.
40	vpn sslvpn users users	System user configuration commands.
41	vpn sslvpn users domains add	Users domain configuration mode
42	vpn sslvpn users domains edit *<ltrow_id>*	Users domain configuration mode
43	vpn sslvpn users domains delete *<ltrow_id>*	Users domain delete mode
44	vpn sslvpn users groups add	Users groups configuration mode
45	vpn sslvpn users groups edit *<ltrow_id>*	Users groups configuration mode
46	vpn sslvpn users groups delete *<ltrow_id>*	Users group delete mode
47	vpn sslvpn users users add	Users configuration mode
48	vpn sslvpn users users edit *<ltrow_id>*	Users configuration mode
49	vpn sslvpn users users login_policies *<ltrow_id>*	Users login policy configuration mode
50	vpn sslvpn users users browser_policies *<ltrow_id>*	Users browsers policy configuration mode
51	vpn sslvpn users users ip_policies	Users ip policy configuration mode
52	vpn sslvpn users users ip_policies configure *<ltrow_id>*	Users ip policy configuration mode
53	vpn sslvpn users users ip_policies delete *<ltrow_id>*	Users ip policy delete mode
54	vpn sslvpn users users delete *<ltrow_id>*	Users delete mode
55	vpn ipsec	vpn policy mode.
56	vpn ipsec policy	vpn policy mode.
57	vpn ipsec policy configure *<ltname>*	vpn policy configuration mode
58	vpn ipsec policy enable *<ltname>*	enable a vpn policy
59	vpn ipsec policy disable *<ltname>*	disable a vpn policy
60	vpn ipsec policy delete *<ltname>*	delete a vpn policy
61	vpn ipsec policy connect *<ltname>*	connect a vpn tunnel
62	vpn ipsec policy drop *<ltname>*	drop a vpn tunnel

7.8 Security configuration commands

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

Sl No	Command Name	Purpose
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 igmp	Security igmp setup.
5	security advanced_network igmp setup	Igmp 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 *<ltrow_id>*	application rules rules configuration mode.
9	security application_rules delete *<ltrow_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 *<ltrow_id>*	custom services configuration mode.
13	security firewall custom_service delete *<ltrow_id>*	custom services configuration mode.
14	security firewall	Firewall rules setup.
15	security firewall ipv4	Firewall IPv4 rules setup.
16	security firewall ipv4 configure	Firewall IPV4 rules configuration mode.
17	security firewall ipv4 default_outbound_policy *<ltdefault_outbound_policy>*	Firewall Settings, Default Outbound Policy configuration mode.
18	security firewall ipv4 edit *<ltrow_id>*	Firewall IPV4 rules configuration mode.
19	security firewall ipv4 enable *<ltrow_id>*	Firewall IPV4 rules configuration mode.
20	security firewall ipv4 disable *<ltrow_id>*	Firewall IPV4 Rules configuration mode.
21	security firewall ipv4 delete *<ltrow_id>*	Firewall IPV4 Rules configuration mode.
22	security firewall ipv4 move *<ltrow_id>*	Firewall IPV4 Rule reordering mode.
23	security firewall algs	Firewall ALGs configuration mode.
24	security firewall ipv6	Firewall IPv6 rules setup.
25	security firewall ipv6 configure	Firewall IPV6 rules configuration mode.
26	security firewall ipv6 edit *<ltrow_id>*	Firewall IPV6 rules configuration mode.
27	security firewall ipv6 enable *<ltrow_id>*	Firewall IPV6 rules configuration mode.
28	security firewall ipv6 disable *<ltrow_id>*	Firewall IPV6 Rules configuration mode.
29	security firewall ipv6 delete *<ltrow_id>*	Firewall IPV6 Rules configuration mode.
30	security firewall ipv6 move *<ltrow_id>*	Firewall IPV6 Rule reordering mode.
31	security firewall ipv6 default_outbound_policy *<ltdefault_outbound_policy>*	Firewall Settings, IPv6 Default Outbound Policy configuration mode.
32	security ids	IDS Configuration setup.
33	security ids configure	IDS configuration mode.
34	security session_settings	Session Settings Configuration setup.
35	security session_settings configure	Session Settings configuration mode.
36	security schedules	Schedules Configuration setup.
37	security schedules add	Schedules configuration mode.
38	security schedules edit *<ltrow_id>*	Schedules configuration mode.
39	security schedules delete *<ltrow_id>*	Schedules configuration mode.
40	security mac_filter	source mac filter configuration mode.
41	security ip_or_mac_binding	ip mac binding configuration mode.
42	security mac_filter configure	source mac filter configuration mode.
43	security mac_filter source	.

44	security mac_filter source add	Source Mac Filter configuration mode.
45	security mac_filter source edit <*ltrow_id*>	Source Mac Filter configuration mode.
46	security mac_filter source delete <*ltrow_id*>	Source Mac Filter configuration mode.
47	security ip_or_mac_binding add	ip/mac binding configuration mode.
48	security ip_or_mac_binding edit <*ltrow_id*>	ip/mac binding configuration mode.
49	security ip_or_mac_binding delete <*ltrow_id*>	ip/mac binding configuration mode.
50	security firewall vpn_passthrough	VPN Passthrough setup.
51	security firewall vpn_passthrough configure	VPN Passthrough configuration mode.
52	security website_filter	website filtering configuration setup.
53	security website_filter content_filtering	content filtering configuration setup.
54	security website_filter approved_urls	trusted domains configuration setup.
55	security website_filter blocked_keywords	blocked keywords configuration setup.
56	security website_filter content_filtering configure	content filtering configuration mode.
57	security website_filter approved_urls add	trusted domains configuration mode.
58	security website_filter approved_urls edit <*ltrow_id*>	trusted domains configuration mode.
59	security website_filter approved_urls delete <*ltrow_id*>	trusted Domains configuration mode.
60	security website_filter blocked_keywords add	blocked Keyword configuration mode.
61	security website_filter blocked_keywords edit <*ltrow_id*>	blocked Keywords configuration mode.
62	security website_filter blocked_keywords delete <*ltrow_id*>	blocked Keywords configuration mode.
63	security website_filter blocked_keywords enable <*ltrow_id*>	blocked Keywords configuration mode.
64	security website_filter blocked_keywords disable <*ltrow_id*>	blocked Keywords configuration mode.

7.9 History configuration commands

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

Sl No	Command Name	Purpose
1	.history <*ltlimit*>	Display the current session's command line history

Chapter 8. Configuration commands WLAN

The configure commands for all the branches mentioned above are discussed in this section.

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

Sl No	Command Name	Purpose
1	w lan ap_management	AP Management
2	w lan ap_management manual	Request administrative commands/actions for managed access points.
3	w lan ap_management ap_database	Enter AP Database configuration mode
4	w lan ap_management rf_management	Configure pow er plan and channel plan related parameters
5	w lan ap_management poll_list	Configure IP address to poll,VLAN ID for L2 discovery or specific discovery method.
6	w lan ap_management poll_list discovery	Configure specific discovery method.
7	w lan ap_management oui_database	Configure Local OUI Database.
8	w lan ap_management manual configure <*macaddr*>	w lan ap_management manual configuration mode
9	w lan ap_management ap_database add <*macaddr*>	w lan ap-management ap-database configuration mode
10	w lan ap_management ap_database edit <*macaddr*>	w lan ap-management ap-database configuration mode
11	w lan ap_management ap_database delete <*macaddr*>	w lan ap-management ap-database delete an mac-address
12	w lan ap_management rf_management configure	w lan ap-management rf-management configuration mode
13	w lan ap_management poll_list configure	w lan ap-management poll-list configuration mode
14	w lan ap_management poll_list delete_ip_address <*ipaddr*>	w lan ap-management ap-database configuration mode
15	w lan ap_management poll_list delete_vlan_list <*id*>	w lan ap-management poll-list delete an vlanid
16	w lan ap_management poll_list discovery configure	w lan ap-management poll-list configuration mode
17	w lan ap_management oui_database add	w lan ap-management oui-database configuration mode
18	w lan ap_management oui_database edit <*ouival*>	w lan ap-management oui-database configuration mode
19	w lan ap_management oui_database delete <*ouival*>	w lan ap-management ap-database delete an oui value
20	w lan ap_profile	Enter the AP Profile configuration mode
21	w lan network	Enter Netw ork configuration mode
22	w lan ap_profile QoS	AP Profile QoS configuration
23	w lan ap_profile radio	AP Profile Radio configuration
24	w lan ap_profile add <*profileid*>	w lan ap_profile configuration mode
25	w lan ap_profile edit <*profileid*>	w lan ap_profile configuration mode
26	w lan ap_profile delete <*profileid*>	Delete a AP Profile
27	w lan ap_profile copy <*sourceprofileid*> <*destprofileid*>	Copy an existing AP profile to a new AP profile
28	w lan ap_profile radio configure <*profileid*> <*radio*>	w lan ap_profile radio configuration mode
29	w lan ap_profile QoS configure <*profileid*> <*radio*>	w lan ap_profile QoS configuration mode
30	w lan network configure <*networkid*>	w lan network configuration mode

31	w lan client	Configure know n client parameters.
32	w lan client add *<macaddr>*	w lan client configuration mode
33	w lan client edit *<macaddr>*	w lan client configuration mode
34	w lan client delete *<macaddr>*	w lan client configuration mode
35	w lan global	Global Configuration
36	w lan global dist_tunnel	Configure the L2 Distributed Tunneling parameters
37	w lan global snmp_trap	Wireless sw itch SNMP trap configuration.
38	w lan global dist_tunnel configure	w lan global distributed tunnel configuration mode
39	w lan global snmp_trap configure	w lan global snmp_trap configuration mode
40	w lan global configure	w lan global configuration mode
41	w lan peer_controller	Configure peer sw itch configuration push groups.
42	w lan peer_controller configure	w lan peer_controller configuration mode
43	w lan peer_controller push_configuration *<ipaddr>*	Start the configuration push for one peer sw itches.
44	w lan w ids_security	Configure the WIDS security parameters.
45	w lan w ids_security ap	Configure the WIDS security parameters for AP
46	w lan w ids_security client	Configure WIDS Client Security Parameters.
47	w lan w ids_security ap configure	w lan w ids_security ap configuration mode
48	w lan w ids_security client configure	w lan w ids_security client configuration mode
49	w lan w lan_global_setting	Wireless Global Configuration
50	w lan w lan_global_setting ap_validation	Configure the AP validation method.
51	w lan w lan_global_setting radius_server	RADIUS related parameters.
52	w lan w lan_global_setting country	country code for the w ireless network
53	w lan w lan_global_setting ap_validation configure	w lan ap_validation configuration mode
54	w lan w lan_global_setting radius_server configure	w lan radius_server configuration mode
55	w lan w lan_global_setting country configure	w lan country configuration mode
56	w lan w lan_global_setting w ireless_switch *<enable>*	Enable/Disable the w ireless switch

8.1 wlan ap_management manual configure <macaddr>

S.No	Command Name	Description	Type and Description
1	*<macaddr>*	w lan ap_management manual configuration mode	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
2	save	Save ap management configuration changes	
3	cancel	Roll back ap management configuration changes.	
4	exit	Save ap management configuration changes and current mode.	
5	radio	Configure radio on a managed access points.	w ireless radio interface
6	channel	Configure managed access points channel value.	Unsigned integer
7	pow er	Enter the transmit pow er	range of pow er perventage
8	debug	Enable/Disble debugging on Managed AP	Boolean choice
9	reset	Reset a WS managed AP.	Boolean choice

8.2 wlan ap_management ap_database add <macaddr>

S.No	Command Name	Description	Type and Description
1	*<macaddr>*	w lan ap-management ap-database configuration mode	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
2	save	Save ap-database configuration changes.	
3	cancel	Roll back ap-database configuration changes.	
4	exit	Save ap-databse configuration changes and current mode.	
5	mode	Configure the AP Managed mode	AP mode
6	location	Configure the AP location description.	String
7	password	Configure the AP Authentication Passw ord.	String
8	profileid	Set the AP Profile ID to use for configuration.	AP Profile ID
9	ssid	Configure the stand-alone AP expected SSID	String
10	channel	Configure the stand-alone AP expected channel	Unsigned integer
11	w ds_mode	Configure the stand-alone AP expected WDS mode	stand-alone AP expected WDS mode.
12	security_mode	Configure the stand-alone AP expected security mode	Stand Alone AP Security Mode
13	w ired-mode	Configure the stand-alone AP expected w ired netw ork mode.	stand-alone AP expected w ired network mode
14	radio1-sentry	Configure fixed radio channel/pow er settings	
15	radio2-802.11b/g/n	Configure fixed radio channel/pow er settings	
16	radio1-sentry channel	Configure a fixed channel for the radio	Unsigned integer
17	radio1-sentry power	Configure a fixed transmit pow er for the radio.	range of pow er perventage
18	radio2-802.11b/g/n channel	Configure a fixed channel for the radio.	Unsigned integer
19	radio2-802.11b/g/n pow er	Configure a fixed transmit pow er for the radio.	range of pow er perventage

8.3 wlan ap_management ap_database edit <macaddr>

S.No	Command Name	Description	Type and Description
1	*<macaddr>*	w lan ap-management ap-database configuration mode	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
2	save	Save ap-database configuration changes.	
3	cancel	Roll back ap-database configuration changes.	
4	exit	Save ap-databse configuration changes and current mode.	
5	mode	Configure the AP Managed mode	AP mode
6	location	Configure the AP location description.	

			String
7	password	Configure the AP Authentication Password.	String
8	profileid	Set the AP Profile ID to use for configuration.	AP Profile ID
9	ssid	Configure the stand-alone AP expected SSID	String
10	channel	Configure the stand-alone AP expected channel	Unsigned integer
11	wds_mode	Configure the stand-alone AP expected WDS mode	stand-alone AP expected WDS mode.
12	security_mode	Configure the stand-alone AP expected security mode	Stand Alone AP Security Mode
13	wired-mode	Configure the stand-alone AP expected wired network mode.	stand-alone AP expected wired network mode
14	radio1-sentry	Configure fixed radio channel/power settings	
15	radio2-802.11b/g/n	Configure fixed radio channel/power settings	
16	radio1-sentry channel	Configure a fixed channel for the radio	Unsigned integer
17	radio1-sentry power	Configure a fixed transmit power for the radio.	range of power perventage
18	radio2-802.11b/g/n channel	Configure a fixed channel for the radio.	Unsigned integer
19	radio2-802.11b/g/n power	Configure a fixed transmit power for the radio.	range of power perventage

8.4 wlan ap_management ap_database delete <macaddr>

S.No	Command Name	Description	Type and Description
1	*<macaddr>*	wlan ap-management ap-database delete an mac-address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

8.5 wlan ap_management rf_management configure

S.No	Command Name	Description	Type and Description
1	save	Save rf management configuration changes.	
2	cancel	Roll back configuration changes.	
3	exit	Save rf management configuration changes and current mode.	
4	channel_plan	Configure the channel plan parameters.	
5	power_plan	Configure the power plan parameters.	
6	channel_plan plan	Specify radio frequency band	Radio frequency Band
7	channel_plan mode	Set the mode of channel plan assignment.	Channel Plan Mode
8	channel_plan history_depth	Configure the number of the channel algorithm iterations that WS remembers.	Unsigned integer
9	channel_plan interval	Configure the interval at which to compute and apply channel adjustments.	Unsigned integer
10	channel_plan time	Configure the scheduled time at which to compute and apply channel adjustments.	String
11	power_plan interval	Configure the interval at which to compute	

		and apply power adjustments.	Unsigned integer
12	power_plan mode	Set the mode of power plan assignment	

8.6 wlan ap_management poll_list configure

S.No	Command Name	Description	Type and Description
1	save	Save poll list configuration changes	
2	cancel	Roll back poll list configuration changes.	
3	exit	Save poll list configuration changes and current mode.	
4	vlan	Configure a VLAN ID for L2 discovery.	vlan id possible values
5	ip_address	Configure IP address to poll.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

8.7 wlan ap_management poll_list delete_ip_address <ipaddr>

S.No	Command Name	Description	Type and Description
1	*<ipaddr>*	wlan ap-management ap-database configuration mode	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

8.8 wlan ap_management poll_list delete_vlan_list <id>

S.No	Command Name	Description	Type and Description
1	*<id>*	wlan ap-management poll-list delete an vlanid	Unsigned integer

8.9 wlan ap_management poll_list discovery configure

S.No	Command Name	Description	Type and Description
1	save	Save poll-list discovery configuration changes	
2	cancel	Roll back poll-list discovery configuration changes.	
3	exit	Save poll-list discovery configuration changes and current mode.	
4	discovery	Enable/Disable specific discovery method.	
5	discovery enable_L2/VLAN	Enable/Disable the discovery of APs and peer switches using L2 multicast frames.	Boolean choice
6	discovery enable_L3/IP	Enable/Disable the discovery of APs and peer switches using IP polling method	Boolean choice

8.10 wlan ap_management oui_database add

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

3	exit	Save discovery oui database changes and current mode.	
4	value	Configure Local OUI Database.	String
5	description	Configure Local OUI Database.	String

8.11 wlan ap_management oui_database edit <ouival>

S.No	Command Name	Description	Type and Description
1	*<ouival>*	w lan ap-management oui-database configuration mode	String
2	save	Save oui database configuration changes	
3	cancel	Roll back oui database configuration changes.	
4	exit	Save discovery oui database changes and current mode.	
5	value	Configure Local OUI Database.	String
6	description	Configure Local OUI Database.	String

8.12 wlan ap_management oui_database delete <ouival>

S.No	Command Name	Description	Type and Description
1	*<ouival>*	w lan ap-management ap-database delete an oui value	String

8.13 wlan ap_profile add <profileid>

S.No	Command Name	Description	Type and Description
1	*<profileid>*	w lan ap_profile configuration mode	AP Profile ID
2	save	Save AP Profile settings.	
3	exit	Save AP Profile settings and exit current mode.	
4	cancel	Roll back AP Profile settings changes.	
5	profile_name	Configure a name for the AP Profile.	String
6	hardw are_type	Configure hardw are type	AP Hardw are Types
7	vlanid	Configure the w ired network detection vlan id	vlan id possible values

8.14 wlan ap_profile edit <profileid>

S.No	Command Name	Description	Type and Description
1	*<profileid>*	w lan ap_profile configuration mode	AP Profile ID
2	save	Save AP Profile settings.	
3	exit	Save AP Profile settings and exit current mode.	

4	cancel	Roll back AP Profile settings changes.	
5	profile_name	Configure a name for the AP Profile.	String
6	hardware_type	Configure hardware type	AP Hardware Types
7	vlanid	Configure the wired network detection vlan id	vlan id possible values

8.15 wlan ap_profile delete <profileid>

S.No	Command Name	Description	Type and Description
1	*<profileid>*	Delete a AP Profile	AP Profile ID

8.16 wlan ap_profile copy <sourceprofileid> <destprofileid>

S.No	Command Name	Description	Type and Description
1	*<sourceprofileid>* *<destprofileid>*	Copy an existing AP profile to a new AP profile	AP Profile ID AP Profile ID

8.17 wlan ap_profile radio configure <profileid> <radio>

S.No	Command Name	Description	Type and Description
1	*<profileid> <radio>*	wlan ap_profile radio configuration mode	AP Profile ID wireless radio interface
2	save	Save AP profile radio settings.	
3	exit	Save AP profile radio settings and exit current mode.	
4	cancel	Roll back AP profile radio settings changes.	
5	mode	Configure the physical mode for the radio interface	
6	state_on	Enable/Disable Station Isolation.	Boolean choice
7	rts_threshold	Configure the RTS threshold	Unsigned integer
8	enable_load_balancing	Enable load balancing parameters for the radio.	Boolean choice
9	load_utilization	Configure the percentage utilization.	range of power perventage
10	maximum_clients	Configure the maximum number of simultaneous client associations allowed.	Unsigned integer
11	rf_scan_otherchannels	Enable/Disable scan of other channels.	Boolean choice
12	rf_scan_sentry	Set the scan mode to sentry.	Boolean choice
13	dtm_period	Configure the DTIM period.	Unsigned integer
14	beacon_interval	Configure the beacon interval	Unsigned integer
15	automatic_channel	Enable/Disable the Automatic Power Save Delivery mode for the radio.	Boolean choice

16	automatic_power	Enable/Disable auto power adjustment	Boolean choice
17	initial_power	Configure a default power setting for the radio.	range of power perventage
18	rate	Configure data rates for the radio	
19	rate basic	Configure basic client rates	Unsigned integer
20	rate supported	Configure supported client rates	Unsigned integer
21	channel_auto_eligble	Enable/Disable channel auto-eligibility for client connections.	Boolean choice

8.18 wlan ap_profile QoS configure <profileid> <radio>

S.No	Command Name	Description	Type and Description
1	*<profileid> <radio>*	wlan ap_profile QoS configuration mode	AP Profile ID wireless radio interface
2	save	Save .	
3	exit	Save and exit current mode.	
4	cancel	Roll back settings changes.	
5	enable_wmm_mode	Enable/Disable WMM mode	Boolean choice
6	edca	Select between AP EDCA parameters or Station EDCA parameters to Configure	AP EDCA parameters or Station EDCA parameters
7	edca_queue	Select which EDCA queue to configure(background,best-effort,video,voice)	EDCA Parameters
8	aifs	Configure the Arbitration Inter-frame Spacing time	Unsigned integer
9	cwmin	Configure the upper limit of the range from which the initial random backoff wait time is determined.	Unsigned integer
10	cwmax	Configure the upper limit for the doubling of the random backoff value.	Unsigned integer
11	max_burst	Configure the maximum burst duration.	Unsigned integer

8.19 wlan network configure <networkid>

S.No	Command Name	Description	Type and Description
1	*<networkid>*	wlan network configuration mode	Unsigned integer
2	save	Save settings.	
3	exit	Save settings and exit current mode.	
4	cancel	Roll back settings changes.	
5	ssid	Configure the SSID for the network.	String
6	hide_ssid	Enable/Disable hiding the SSID for the network.	Boolean choice
7	ignore_broadcast	Enable/Disable deny broadcast mode for the network.	Boolean choice
8	vlan	Configure the default VLAN ID.	Unsigned integer
9	mac_authentication	Configure client MAC authentication parameters.	wireless ap validation type

10	redirect_mode	Configure the redirect mode for the netw ork	netw ork redirect mode
11	redirect_url	Configure the HTTP redirect URL for the netw ork	String
12	arp_suppression	Enable/Disable Wireless ARP Suppression for the netw ork.	Boolean choice
13	dist_tunnel	Enable/Disable distributed tunneling mode for the netw ork.	Boolean choice
14	radius_parm	Configure RADIUS related parameters	
15	radius_parm accounting	Enable/Disable RADIUS accounting function.	Boolean choice
16	radius_parm server_name	Configure Authentication/Accounting RADIUS Server Name	
17	radius_parm server_name auth	Configure Authentication RADIUS Server Name	String
18	radius_parm server_name acct	Configure Accounting RADIUS Server Name	String
19	radius_parm use_netw ork_configuration	Enable/Disable override of Netw ork RADIUS configuration	Boolean choice

8.20 wlan client add <macaddr>

S.No	Command Name	Description	Type and Description
1	*<macaddr>*	w lan client configuration mode	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
2	save	Save client configuration changes.	
3	cancel	Roll back client configuration changes.	
4	exit	Save client configuration changes and current mode.	
5	name	Configure a Know n Client name.	String
6	action	Configure a Know n Client authentication action.	Know n Client Authentication Action

8.21 wlan client edit <macaddr>

S.No	Command Name	Description	Type and Description
1	*<macaddr>*	w lan client configuration mode	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
2	save	Save client configuration changes.	
3	cancel	Roll back client configuration changes.	
4	exit	Save client configuration changes and current mode.	
5	name	Configure a Know n Client name.	String
6	action	Configure a Know n Client authentication action.	Know n Client Authentication Action

8.22 wlan client delete <macaddr>

S.No	Command Name	Description	Type and Description
1	*<macaddr>*	w lan client configuration mode	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF

8.23 wlan global dist_tunnel configure

S.No	Command Name	Description	Type and Description
1	save	Save Distributed Tunneling settings.	
2	exit	Save Distributed Tunneling settings and exit current mode.	
3	cancel	Roll back Distributed Tunneling settings changes.	
4	max_clients	Enter maximum client connections supported.	Unsigned integer
5	idle_timeout	Enter idle timeout value in seconds.	Unsigned integer
6	max_timeout	Enter maximum timeout value in seconds	Unsigned integer
7	mcast_reply	Enter maximum multicast relplications allow ed.	Unsigned integer

8.24 wlan global snmp_trap configure

S.No	Command Name	Description	Type and Description
1	save	Save SNMP Trap settings.	
2	exit	Save SNMP Trap settings and exit current mode.	
3	cancel	Roll back SNMP Trap settings changes.	
4	ap_failure	Enable/Disable SNMP traps for AP association/authentication failures.	Boolean choice
5	ap_state	Enable/Disable SNMP traps for AP state changes.	Boolean choice
6	client_failure	Enable/Disable SNMP traps for client association/authentication failures.	Boolean choice
7	client_state	Enable/Disable SNMP traps client state changes	Boolean choice
8	peer_w s	Enable/Disable SNMP traps for peer w lan sw itch events.	Boolean choice
9	rf_scan	Enable/Disable SNMP traps for RF scan related events.	Boolean choice
10	rogue_ap	Enable/Disable SNMP traps for rogue access points.	Boolean choice
11	tspec	Enable/Disable SNMP traps for TSPEC related events.	Boolean choice
12	w ids_status	Enable/Disable SNMP traps for WIDS status events.	Boolean choice
13	w s_status	Enable/Disable SNMP traps for w s status events	Boolean choice

8.25 wlan global configure

S.No	Command Name	Description	Type and Description

1	save	Save WLAN Global settings.	
2	exit	Save WLAN Global Configuration and exit current mode.	
3	cancel	Roll back WLAN Global settings changes.	
4	peer_group_id	Configure the peer switch group ID	Unsigned integer
5	client_roam_timeout	Configure client roam timeout	Unsigned integer
6	ad_hoc_client_timeout	Configure entry age for ad hoc network status	Unsigned integer
7	ap_failure_status_timeout	Configure entry age for AP failure status.	Unsigned integer
8	mac_authentication_mode	Configure the MAC Authentication Mode	MAC Authentication mode
9	rf-scan_status_timeout	Configure entry age for RF scan status	Unsigned integer
10	detected_client_status_timeout	Configure entry age for detected clients status	Unsigned integer
11	tunnel_ip_mtu_size	Configure the Tunnel MTU.	MAC Authentication mode
12	cluster_priority	Configure the Cluster Priority.	Unsigned integer
13	enable_ap_client_QoS	Enable/Disable AP QoS for wlan clients	Boolean choice

8.26 wlan peer_controller configure

S.No	Command Name	Description	Type and Description
1	save	Save peer controller configuration changes.	
2	cancel	Roll back peer controller configuration changes.	
3	exit	Save peer controller configuration changes and current mode.	
4	enable_global	Enable/Disable global configuration push to peer switches.	Boolean choice
5	enable_discovery	Enable/Disable discovery configuration push to peer switches.	Boolean choice
6	enable_channel/power	Enable/Disable channel and power configuration push to peer switches.	Boolean choice
7	enable_ap_database	Enable/Disable AP database configuration push to peer switches.	Boolean choice
8	enable_device_location	Enable/Disable device location configuration push to peer switches.	Boolean choice
9	enable_ap_profile	Enable/Disable AP profile and network configuration push to peer switches.	Boolean choice
10	enable_known_client	Enable/Disable known client configuration push to peer switches.	Boolean choice
11	enable_captive_portal	Enable/Disable Captive Portal configuration push to peer switches.	Boolean choice
12	enable_radius_client	Enable/Disable RADIUS client configuration push to peer switches.	Boolean choice
13	enable_QoS_acl	Enable/Disable QoS ACL configuration push to peer switches.	Boolean choice
14	enable_QoS_diffserv	Enable/Disable QoS DiffServ configuration push to peer switches	Boolean choice
15	enable_wds_group	Enable/Disable wds group configuration push to peer switches.	Boolean choice

8.27 wlan peer_controller push_configuration <ipaddr>

S.No	Command Name	Description	Type and Description
1	*<ipaddr>*	Start the configuration push for one peer switches.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

8.28 wlan wids_security ap configure

S.No	Command Name	Description	Type and Description
1	save	Save Wids Security settings.	
2	exit	Save Configurable wids security settings and exit current mode.	
3	cancel	Roll back Configurable wids security settings changes.	
4	admin_config_rogue	Enable Rogue reporting for admin configured Rogue AP's.	Boolean choice
5	ap_chan_illegal	Enable or disable Rogue reporting for AP's is operating on an illegal channel.	Boolean choice
6	ap_de_auth_attack	Enable or disable the AP de-authentication attack.	Boolean choice
7	fakeman_ap_chan_invalid	Enable or disable Rogue reporting for fake managed AP's detected with an invalid channel.	Boolean choice
8	fakeman_ap_managed_ssid	Enable or disable Rogue reporting for fake managed AP's detected with a managed SSID.	Boolean choice
9	fakeman_ap_no_ssid	Enable or disable Rogue reporting for APs detected with no SSID.	Boolean choice
10	managed_ap_ssid_invalid	Enable or disable Rogue reporting for managed AP's detected with an invalid SSID.	Boolean choice
11	managed_ssid_secu_bad	Enable or disable Rogue reporting for AP's detected with managed SSID's and an invalid security configuration.	Boolean choice
12	standalone_cfg_invalid	Enable or disable Rogue reporting for standalone AP's operating with unexpected configuration.	Boolean choice
13	unknown_ap_managed_ssid	Enable or disable Rogue reporting for unknown AP's detected with a managed SSID.	Boolean choice
14	unmanaged_ap_wired	Enable or disable Rogue reporting for unmanaged AP's on a wired network	Boolean choice
15	rogue_det_trap_interval	Configure the Rogue detected trap interval.	Unsigned integer
16	wired_detection_interval	Configure the wired network detection interval.	Unsigned integer
17	wds_device_unexpected	Enable or disable Rogue reporting for detection of unexpected WDS devices.	Boolean choice

8.29 wlan wids_security client configure

S.No	Command Name	Description	Type and Description
1	save	Save wids client settings.	
2	exit	Save wids client settings and exit current mode.	
3	cancel	Roll back wids client settings changes.	
4	auth_with_unknown_ap	Enable or Disable the Known Client is authenticated with unknown AP test	Boolean choice

5	configured_auth_rate	Enable or Disable the configured rate of 802.11 Auth Requests test.	Boolean choice
6	configured_deauth_rate	Enable or Disable the configured rate of 802.11 Deauth Requests test.:	Boolean choice
7	configured_probe_rate	Enable or Disable the configured rate of 802.11 Probe Requests test.	Boolean choice
8	known_client_database	Enable or Disable the client present in Known DB Test	Boolean choice
9	max_auth_failure	Enable or Disable the Maximum number of Authentication Failures test.	Boolean choice
10	oui_database	Enable or Disable the client present in OUI DB Test.	Boolean choice
11	threat_mitigation	Enable or Disable Client Threat Mitigation.	Boolean choice
12	known_db_location	Configure the Known Client database location.	wireless ap validation type
13	known_db_radius_server_name	Configure the Known Client database server name	String
14	rogue_det_trap_interval	Set the Rogue Detection Trap Interval	Unsigned integer
15	threshold_interval_deauth	Configure the De-Authentication Requests Threshold Interval.	Unsigned integer
16	threshold_value_deauth	Configure the De-Authentication Requests Threshold Value	Unsigned integer
17	threshold_value_auth	Configure the Authentication Requests Threshold Value.	Unsigned integer
18	threshold_interval_probe	Configure the Probe Requests Threshold Value.	Unsigned integer
19	threshold_value_probe	Configure the Probe Requests Threshold Value	Unsigned integer
20	threshold_auth_failure	Configure the Authentication Failures Threshold Value.	Unsigned integer

8.30 wlan wlan_global_setting ap_validation configure

S.No	Command Name	Description	Type and Description
1	save	Save ap validation configuration changes.	
2	cancel	Roll back ap validation configuration changes.	
3	exit	Save ap validation configuration changes and current mode.	
4	validation	Use local AP database or configured RADIUS server to validate discovered APs	wireless ap validation type
5	authentication	Enable/Disable AP authentication mode.	Boolean choice

8.31 wlan wlan_global_setting radius_server configure

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

3	exit	Save radius server configuration changes and current mode.	
4	authentication_server_name	Configure Authentication RADIUS Server Name	String
5	accounting_server_name	Configure Accounting RADIUS Server Name	String
6	accounting_enable	Enable/Disable RADIUS accounting function	Boolean choice

8.32 wlan wlan_global_setting country configure

S.No	Command Name	Description	Type and Description
1	save	Save country configuration changes.	
2	cancel	Roll back country configuration changes.	
3	exit	Save country configuration changes and current mode.	
4	country	Enter a country code	

8.33 wlan wlan_global_setting wireless_switch <enable>

S.No	Command Name	Description	Type and Description
1	*<enable>*	Enable/Disable the wireless switch	Boolean choice

8.34 wlan wlan_global_setting wireless_switch <enable>

S.No	Command Name	Description	Type and Description
1	*<enable>*	Enable/Disable the wireless switch	Boolean choice

Chapter 9. Configuration commands System

9.1 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_Option_accept_packet_logs	lan to Option accepted Pkts Enable/Disable	Boolean choice
5	lan_Option_drop_packet_logs	lan to Option dropped Pkts Enable/Disable	Boolean choice
6	Option_lan_accept_packet_logs	Option to lan accepted Pkts logs Enable/Disable	Boolean choice
7	Option_lan_drop_packet_logs	Option to lan dropped Pkts logs Enable/Disable	Boolean choice
8	Option_dmz_accept_packet_logs	Option to dmz accepted Pkts logs Enable/Disable	Boolean choice
9	Option_dmz_drop_packet_logs	Option to dmz dropped Pkts logs Enable/Disable	Boolean choice
10	dmz_Option_accept_packet_logs	dmz to Option accepted Pkts logs Enable/Disable	Boolean choice
11	dmz_Option_drop_packet_logs	dmz to Option 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	source_mac_filter_logs	Source mac filter logs Enable/Disable	Boolean choice
19	bandwidth_limit_logs	Bandwidth Limit logs Enable/Disable	Boolean choice
20	ftp_logs	FTP logs Enable/Disable	Boolean choice
21	icmp_invalid_logs	Invalid ICMP Packets logs Enable/Disable	Boolean choice
22	icmp_redirect_logs	Redirected ICMP Packets logs Enable/Disable	Boolean choice
23	log_invalid_packet	Log invalid packet Enable/Disable	Boolean choice

9.2 system logging ipv4 configure

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

9.3 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 w hether or not system emails scheduled logs.	Boolean choice
6	email_server	Set options for emailing of logs.	String
7	return_email	Set email address SMTP server replies are sent.	String
8	send_to_email	Set email address w here logs and alerts w ill be sent.	String
9	smtp_auth	Set SMTP authentication details.	
10	smtp_auth type	Set SMTP authentication types.	SMTP Authentication Types.
11	smtp_auth username	Set SMTP authentication username (for plain and CRAM-MD5 auth).	String
12	smtp_auth password	Set SMTP authentication password (for plain and CRAM-MD5 auth).	String
13	identd_from_smtp_server_enable	Enable/Diable to identd from smtp server.	Boolean choice
14	schedule	Set schedule for sending log by email.	
15	schedule unit	Set schedule unit.	Schedule Unit Types.
16	schedule day	Set schedule day.	Schedule Day Types.
17	schedule time	Set schedule time.	Schedule Time Units Types.
18	schedule meridiem	Set schedule meridiem.	Schedule Meridiem Types.
19	syslog_server	syslog	
20	syslog_server server_name1	server1	
21	syslog_server server_name2	server2	

22	syslog_server server_name3	server3	
23	syslog_server server_name4	server4	
24	syslog_server server_name5	server5	
25	syslog_server server_name6	server6	
26	syslog_server server_name7	server7	
27	syslog_server server_name8	server8	
28	syslog_server server_name1 enable	Boolean Choice Y/N	Boolean choice
29	syslog_server server_name1 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
30	syslog_server server_name1 severity	Set Syslog severity.	syslog server severity types
31	syslog_server server_name1 facility	Set Syslog facility.	syslog server facility ID types
32	syslog_server server_name2 enable	Boolean Choice Y/N	Boolean choice
33	syslog_server server_name2 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
34	syslog_server server_name2 severity	Set Syslog severity.	syslog server severity types
35	syslog_server server_name2 facility	Set Syslog facility.	syslog server facility ID types
36	syslog_server server_name3 enable	Boolean Choice Y/N	Boolean choice
37	syslog_server server_name3 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
38	syslog_server server_name3 severity	Set Syslog severity.	syslog server severity types
39	syslog_server server_name3 facility	Set Syslog facility.	syslog server facility ID types
40	syslog_server server_name4 enable	Boolean Choice Y/N	Boolean choice
41	syslog_server server_name4 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
42	syslog_server server_name4 severity	Set Syslog severity.	syslog server severity types
43	syslog_server server_name4 facility	Set Syslog facility.	syslog server facility ID types
44	syslog_server server_name5 enable	Boolean Choice Y/N	Boolean choice
45	syslog_server server_name5 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
46	syslog_server server_name5 severity	Set Syslog severity.	syslog server severity types
47	syslog_server server_name5 facility	Set Syslog facility.	syslog server facility ID types

48	syslog_server server_name6 enable	Boolean Choice Y/N	Boolean choice
49	syslog_server server_name6 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
50	syslog_server server_name6 severity	Set Syslog severity.	syslog server severity types
51	syslog_server server_name6 facility	Set Syslog facility.	syslog server facility ID types
52	syslog_server server_name7 enable	Boolean Choice Y/N	Boolean choice
53	syslog_server server_name7 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
54	syslog_server server_name7 severity	Set Syslog severity.	syslog server severity types
55	syslog_server server_name7 facility	Set Syslog facility.	syslog server facility ID types
56	syslog_server server_name8 enable	Boolean Choice Y/N	Boolean choice
57	syslog_server server_name8 name	Set Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
58	syslog_server server_name8 severity	Set Syslog severity.	syslog server severity types
59	syslog_server server_name8 facility	Set Syslog facility.	syslog server facility ID types

9.4 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_Option_accept_enable	Enable/Disable logging for the LAN to Option Accept packets	Boolean choice
5	lan_Option_drop_enable	Enable/Disable logging for the LAN to option Dropped packets	Boolean choice
6	Option_lan_accept_enable	Enable/Disable logging for the option to LAN Accept packets	Boolean choice
7	Option_lan_drop_enable	Enable/Disable logging for the Option to LAN Dropped packets	Boolean choice

9.5 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
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	Status	Enable/disable remote snmp.	Boolean choice

9.6 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

9.7 system snmp trap configure <*ltagent_ip*>

S.No	Command Name	Description	Type and Description
1	<ltagent_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.	
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	String
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

9.8 system snmp trap delete <*ltagent_ip*>

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

9.9 system snmp users configure <*ltuser*>

S.No	Command Name	Description	Type and Description
1	<ltuser>	SNMP v3 User list configuration changes	snmpv3uers 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	snmpv3uers list authentication algorithm type
7	privacy_algorithm	DES-56 privacy is available for the authentication negotiation	snmpv3uers 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

9.10 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

9.11 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	agent	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DDD 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.DDD where each part is in the range 0-255
6	accessType	SNMP trap port the trap messages will be sent to.	String
7	community	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community	String

9.12 system snmp access edit <*ltrowid*>

S.No	Command Name	Description	Type and Description
1	<ltrow id>	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	agent	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DDD 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.DDD where each part is in the range 0-255
7	accessType	SNMP trap port the trap messages will be sent to.	String
8	community	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community	String

9.13 system snmp access delete <*ltrowid*>

S.No	Command Name	Description	Type and Description
1	<ltrow id>	snmp access configuration mode	Unsigned integer

9.14 system switch_settings power_saving configure

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

9.15 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

9.16 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	timezone	Timezone	Timezones
5	auto_daylight	Specify whether system automatically adjusts for daylight savings time	Boolean choice
6	configure_ntp_servers	Specify whether to use ntpp servers or user will set date and time	Boolean choice
7	use_default_servers	Specify whether to use system default NTP servers.	Boolean choice
8	ntp_server1	Set NTP server#1.	String
9	ntp_server2	Set NTP server#2	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 seconds for the date	Unsigned integer

9.17 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
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

9.18 system usb usb1 configure

S.No	Command Name	Description	Type and Description
1	save	Save Configurable OPTION settings.	
2	exit	Save configurable OPTION settings and exit current mode.	
3	cancel	Roll back Configurable OPTION 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	Select the USB type 3G_USB_ADAPTOR/USB_Disc	usb device type

9.19 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.	
3	cancel	Roll back Configurable OPTION 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	Select the USB type 3G_USB_ADAPTOR/USB_Disc	usb device type

9.20 system groups configure

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	String
5	description	Enter a brief description of the group here	String
6	capabilities	The comma separated list of usertype numeric codes.: SSLVPN:0 Admin:3 Guest:4 L2TP:7 PPTP:8 Local:9 CaptivePortal:10	String
7	grouptimeOut	Enter the time out for group	Unsigned integer

9.21 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	String
5	description	Enter a brief description of the group here	String
6	capabilities	The comma separated list of usertype numeric codes.: SSLVPN:0 Admin:3 Guest:4 L2TP:7 PPTP:8 Local:9 CaptivePortal:10	String
7	grouptimeOut	Enter the time out for group	Unsigned integer

9.22 system group edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	groupname	Enter the Group Name here	String
6	description	Enter a brief description of the group here	String
7	capabilities	The comma separated list of usertype numeric codes.: SSLVPN:0 Admin:3 Guest:4 L2TP:7 PPTP:8 Local:9 CaptivePortal:10	String
8	grouptimeOut	Enter the time out for group	Unsigned integer

9.23 system group delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	system groups delete mode.	Unsigned integer

9.24 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	String
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	usertimeout	Enter the time out for group	Unsigned integer

9.25 system users edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	username	Enter the username here	String
6	FirstName	Enter the user's first name here	String
7	LastName	Enter the user's last name here	String
8	password	Enter the password here	String
9	password_confirm	Re-Enter the password here	String
10	groupname	Enter the groupname here	String
11	usertimeout	Enter the time out for group	Unsigned integer

9.26 system users delete <ltrow_id>

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

9.27 system users password <ltuser>

S.No	Command Name	Description	Type and Description
1	*<ltuser>*	Change password.	String

9.28 system users idle_timeout <lttimeout>

S.No	Command Name	Description	Type and Description

1	*<lttimeout>*	Change idle timeout.	Unsigned integer

9.29 system group groupaccesscontrol configure <ltgroup_id>

S.No	Command Name	Description	Type and Description
1	*<ltgroup_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	login_timeout	login timeout	idle timeout value for user.
6	lockout_enable	lockout enable	Boolean choice
7	max_lockout_attempts	max lockout attempts	Unsigned integer
8	lock_period	lock period	Unsigned integer
9	deny_login	deny login	Boolean choice
10	deny_login_Option	deny login Option	Boolean choice
11	allow _login_from_defined_ips	login fromip	Boolean choice
12	allow _login_from_defined_browsers	login frombrowser	Boolean choice

9.30 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 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

9.31 system group access_control_browser delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Delete a browser fromAccess Control browsers list	Unsigned integer

9.32 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

9.33 system group access_control_ip delete <ltrow_id>

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

Chapter 10. Configuration commands UTIL

10.1 util system_check ping <ltip_address>

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

10.2 util system_check dns_lookup <ltdns>

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

10.3 util system_check traceroute <ltip_address>

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

10.4 util system_check capturePackets start <ltinterface>

S.No	Command Name	Description	Type and Description
1	*<ltinterface>*	Start the packet capture	OPTION interface type

10.5 util system_check capturePackets download <ltfileName> <ltipAddr>

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

10.6 util cat <ltfileName>

S.No	Command Name	Description	Type and Description
1	*<ltfileName>*	Concatenate files and print on the standard output.	String

10.7 util md5sum <ltfileName>

S.No	Command Name	Description	Type and Description
1	*<ltfileName>*	Compute and check MD5 message digest.	String

10.8 util copy <ltfileName1> <ltfileName2>

S.No	Command Name	Description	Type and Description
1	*<ltfileName1> <ltfileName2>*	Copy the Files.	String String

10.9 util usb_test <ltipAddr> <ltfileName>

S.No	Command Name	Description	Type and Description
1	*<ltipAddr> <ltfileName>*	To test the USB.	String String

Chapter 11. Configure commands QOS

11.1 qos lan status

S.No	Command Name	Description
1	lan status	display status of lan qos
2	lan enable	enable qos on lan
3	lan disable	disable qos on lan
4	lan trustmode	configure trustmode configuration in the switch
5	lan trustmode status	show the trust mode configuration on the switch
6	lan trustmode cos	configure cos based qos on a switch port
7	lan trustmode dscp	configure dscp based qos on a switch port
8	lan cos-map	configures the cos-map for the switch port
9	lan trustmode cos enable	configures trustmode cos based qos on lan
10	lan trustmode dscp enable	configures trustmode as dscp qos on lan
11	lan cos-map show	show the cos-map for the for LAN
12	lan cos-map configure	configure cos map for qos
13	lan dscp-map	configures the dscp-map for switch
14	lan dscp-map show	display dscp priority mappin on switch
15	lan dscp-map configure	configure dscp map for qos
16	lan cos-to-dscp-remarking enable	enables cos-to-dscp remarking
17	lan cos-to-dscp-remarking disable	disables cos-to-dscp remarking
18	lan queue	queue sheduling and management configuration
19	lan queue management	lan queue managenet configuation
20	lan queue management show	queue management configuation show
21	lan queue scheduling-algo	configure queue-scheduling-algo
22	lan queue scheduling-algo set	set the queue scheduling algorithm in the LAN switch
23	lan queue scheduling-algo show	show the queue scheduling algo in the LAN switch
24	lan cos-to-dscp-remarking configure	disables cos-to-dscp remarking
25	option status	display status of option qos
26	option enable	enable qos on option
27	option disable	disable qos on option interface
28	option bandwidth	set the bandwidth for option interface
29	option bandwidth set	set the bandwidth for option interface
30	option bandwidth show	show the bandwidth for option interface
31	option bw-profile add	add a bandwidth profile
32	option bw-profile del	delete a bandwidth profile
33	option traffic-selector	Traffic selector configuration
34	option traffic-selector add	add a traffic selector for option
35	option traffic-selector add ip	add a traffic selector for option
36	option traffic-selector add mac	add a traffic selector for option
37	option traffic-selector add port	add a traffic selector for option
38	option traffic-selector add vlan	add a traffic selector for option
39	option traffic-selector add dscp	add a traffic selector for option
40	option traffic-selector del	delete a traffic selector rule for option

11.2 qos lan trustmode cos enable <ltlanPort>

S.No	Command Name	Description

1	*<ltlanPort>*	configures CoS LAN, QoS has to be enabled first.

11.3 qos lan trustmode dscp enable <ltlanPort>

S.No	Command Name	Description
1	*<ltlanPort>*	configures DSCP on LAN, QoS has to be enabled first.

11.4 qos lan cos-map configure <ltcosValue> <ltpriorityQueue>

S.No	Command Name	Description
1	*<ltcosValue> <ltpriorityQueue>*	configure cos map for qos

11.5 qos lan dscp-map configure <ltdscpValue> <ltpriorityQueue>

S.No	Command Name	Description
1	*<ltdscpValue> <ltpriorityQueue>*	Configure DSCP map for qos

11.6 qos lan cos-to-dscp-remarking enable

S.No	Command Name	Description
1	lan status	display status of lan qos
2	lan enable	enable qos on lan
3	lan disable	disable qos on lan
4	lan trustmode	configure trustmode configuration in the switch
5	lan trustmode status	show the trust mode configuration on the switch
6	lan trustmode cos	configure cos based qos on a switch port
7	lan trustmode dscp	configure dscp based qos on a switch port
8	lan cos-map	configures the cos-map for the switch port
9	lan trustmode cos enable	configures trustmode cos based qos on lan
10	lan trustmode dscp enable	configures trustmode as dscp qos on lan
11	lan cos-map show	show the cos-map for the for LAN
12	lan cos-map configure	configure cos map for qos
13	lan dscp-map	configures the dscp-map for switch
14	lan dscp-map show	display dscp priority mappin on switch
15	lan dscp-map configure	configure dscp map for qos
16	lan cos-to-dscp-remarking enable	enables cos-to-dscp remarking
17	lan cos-to-dscp-remarking disable	disables cos-to-dscp remarking
18	lan queue	queue sheduling and management configuration
19	lan queue management	lan queue managenet configuation
20	lan queue management show	queue management configuation show
21	lan queue scheduling-algo	configure queue-scheduling-algo
22	lan queue scheduling-algo set	set the queue scheduling algorithm in the LAN switch
23	lan queue scheduling-algo show	show the queue scheduling algo in the LAN switch
24	lan cos-to-dscp-remarking configure	disables cos-to-dscp remarking
25	option status	display status of option qos
26	option enable	enable qos on option
27	option disable	disable qos on option interface
28	option bandwidth	set the bandwidth for option interface
29	option bandwidth set	set the bandwidth for option interface

30	option bandwidth show	show the bandwidth for option interface
31	option bw-profile add	add a bandwidth profile
32	option bw-profile del	delete a bandwidth profile
33	option traffic-selector	Traffic selector configuration
34	option traffic-selector add	add a traffic selector for option
35	option traffic-selector add ip	add a traffic selector for option
36	option traffic-selector add mac	add a traffic selector for option
37	option traffic-selector add port	add a traffic selector for option
38	option traffic-selector add vlan	add a traffic selector for option
39	option traffic-selector add dscp	add a traffic selector for option
40	option traffic-selector del	delete a traffic selector rule for option

11.7 qos lan cos-to-dscp-remarking configure <ltcosValue> <ltdscpValue>

S.No	Command Name	Description
1	*<ltcosValue> <ltdscpValue>*	configures cos-to-dscp remarking

11.8 qos option bandwidth set <ltwanInterface> <ltupStreamBW> <ltdownStreamBW>

S.No	Command Name	Description	Type and Description
1	*<ltwanInterface> <ltupStreamBW> <ltdownStreamBW>*	set the bandwidth for optional option	OPTION interface type Maximum bandwidth rate 100-100000 Kbps Maximum bandwidth rate 100-100000 Kbps

11.9 16 qos option bandwidth profile add <ltwanInterface> <ltbwProfileName> <ltpriority> <ltmaxBW> <ltminBW>

S.No	Command Name	Description	Type and Description
1	*<ltwanInterface> <ltbwProfileName> <ltpriority> <ltmaxBW> <ltminBW>*	add a bw-profile for option	OPTION interface type String, Max 128 characters and no ' or empty space or " Priority of the traffic Maximum bandwidth rate 100-100000 Kbps Maximum bandwidth rate 100-100000 Kbps

11.10 qos option bandwidth profile del <ltbwProfileName>

S.No	Command Name	Description	Type and Description
1	*<ltbwProfileName>*	delete a bw-profile on option	String, Max 128 characters and no ' or empty space or "

11.11 qos option traffic-selector add ip <ltipAddress> <ltservice> <ltbwProfile>

S.No	Command Name	Description	Type and Description
1	*<ltipAddress> <ltservice> <ltbwProfile>*	add a traffic selector for option	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 service type String, Max 128 characters and no ' or empty space or "

11.12 qos option traffic-selector add mac <ltmacAddress> <ltservice> <ltbwProfile>

S.No	Command Name	Description	Type and Description
1	*<ltmacAddress> <ltservice> <ltbwProfile>*	add a traffic selector for option	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF service type String, Max 128 characters and no ' or empty space or "

11.13 qos option traffic-selector add port <ltlanPort> <ltservice> <ltbwProfile>

S.No	Command Name	Description	Type and Description
1	*<ltlanPort> <ltservice> <ltbwProfile>*	add a traffic selector for option	traffic selectors Port types service type String, Max 128 characters and no ' or empty space or "

11.14 qos option traffic-selector add vlan <ltvlanId> <ltservice> <ltbwProfile>

S.No	Command Name	Description	Type and Description
1	*<ltvlanId> <ltservice> <ltbwProfile>*	add a traffic selector for option	VLAN ID Range Types service type String, Max 128 characters and no ' or empty space or "

11.15 qos option traffic-selector add dscp <ltdscpId> <ltservice> <ltbwProfile>

S.No	Command Name	Description	Type and Description
1	*<ltdscpId> <ltservice> <ltbwProfile>*	add a traffic selector for option	DSCP value to be configured. service type String, Max 128 characters and no ' or empty space or "

11.16 qos option traffic-selector del <lttrafficSelectorId>

S.No	Command Name	Description
1	*<lttrafficSelectorId>*	delete a traffic selector for option

11.17 qos lan queue scheduling-algo set <ltsched-algo>

S.No	Command Name	Description
1	*<ltsched-algo>*	set the queue scheduling algorithm in the LAN switch

Chapter 12. Configuration commands NET

12.1 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 Option IPv4 network to reach an IPV6 network.	Boolean choice

12.2 net ddns Option1 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	enable	Enable or disable Dyndns to provide Dynamic DNS service	Boolean choice
5	hostname	Set Hostname.	String
6	username	Set username.	String
7	password	Set Password.	String
8	time_update_enable	Set Timeperiod as 30 days.	Boolean choice
9	wild_flag_enable	Enable / Disable using wild cards.	Boolean choice

12.3 net ddns Option2 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	enable	Enable or disable Dyndns to provide Dynamic DNS service	Boolean choice
5	hostname	Set Hostname.	String
6	username	Set username.	String
7	password	Set Password.	String
8	time_update_enable	Set Timeperiod as 30 days.	Boolean choice
9	wild_flag_enable	Enable / Disable using wild cards.	

			Boolean choice

12.4 net lan dhcp reserved_ip configure <ltmac_address>

S.No	Command Name	Description	Type and Description
1	*<ltmac_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

12.5 net lan dhcp reserved_ip delete <ltmac_address>

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

12.6 net Option dhcpc configure

S.No	Command Name	Description	Type and Description
1	save	Save dhcpc configuration changes.	
2	cancel	Roll back dhcpc configuration changes.	
3	exit	Save dhcpc configuration changes and current mode.	
4	GetDnsFromIspEnable	Enable/Disable Get DNS Automatically from ISP	Boolean choice
5	PrimaryDns	Set Primary DNS server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	SecondaryDns	Set Secondary DNS server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12.7 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	ip_address	Static IP address.	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	dhcp_mode	Set DHCP mode.	dhcpv4 modes
7	starting_ip_address	DHCP Starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	ending_ip_address	DHCP ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	primary_dns_server	Primary DNS address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	secondary_dns_server	Secondary DNS server address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	wins_server	Set DHCP WINS server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	lease_time	Set DHCP lease time.	Unsigned integer
13	relay_gateway	Set DHCP Relay gateway server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	dns_proxy_enable	Set DNS proxy Enable/Disable.	Boolean choice
15	enable_ldap	Enable/Disable LDAP Server Info.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12.8 net dmz dhcp reserved_ip configure <ltmac_address>

S.No	Command Name	Description	Type and Description
1	*<ltmac_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

12.9 net dmz dhcp reserved_ip delete <ltmac_address>

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

12.10 net ethernet configure <ltinterface_name>

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

12.11 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
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 ist 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
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

12.12 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
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

12.13 net lan ipv6 pool configure <ltipv6PoolStartAddr>

S.No	Command Name	Description	Type and Description
1	*<ltipv6PoolStartAddr>*	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

12.14 net lan ipv6 pool delete <ltipv6PoolStartAddr>

S.No	Command Name	Description	Type and Description
1	*<ltipv6PoolStartAddr>*	IPv6 LAN configuration delete.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.15 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	Option_hosts	IntelAmt Option Host Type.	Intel Amt Option Host type
6	Option_host_Address	IntelAmt option Host Address	String
7	Internal_Address	IntelAmt intenal Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

12.16 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_destport	enable intelamt reflectors on different ports	
7	enable Intel_Amt_Reflector_destport 16992	enable/disable Ports.	Boolean choice
8	enable Intel_Amt_Reflector_destport 16993	enable/disable Ports.	Boolean choice
9	enable Intel_Amt_Reflector_destport 16994	enable/disable Ports.	Boolean choice
10	enable Intel_Amt_Reflector_destport 16995	enable/disable Ports.	Boolean choice

11	enable Intel_Amt_Reflector_destport 9971	enable/disable Ports.	Boolean choice
12	Intel_Amt_Reflector_srcport	set port number for different ports	
13	Intel_Amt_Reflector_srcport 16992	Enter source port value for 16992	Port number
14	Intel_Amt_Reflector_srcport 16993	Enter source port value for 16993	Port number
15	Intel_Amt_Reflector_srcport 16994	Enter source port value for 16994	Port number
16	Intel_Amt_Reflector_srcport 16995	Enter source port value for 16995	Port number
17	Intel_Amt_Reflector_srcport 9971	Enter source port value for 9971	Port number

12.17 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 Aias server configuration changes and exit current mode.	
4	Interface	Select the Interface for the Ip Aliasing	OPTION 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
6	Subnet_Mask	Subnet mask for ip Aliasing	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12.18 net ip_Aliasing server edit <Itrow_id>

S.No	Command Name	Description	Type and Description
1	*<Itrow_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 Aias server configuration changes and exit current mode.	
5	Interface	Select the Interface for the Ip Aliasing	OPTION 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

12.19 net ip_Aliasing server delete <Itrow_id>

S.No	Command Name	Description	Type and Description
1	*<Itrow_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 Aias server configuration changes and exit current mode.	
5	Interface	Select the Interface for the Ip Aliasing	OPTION interface type
6	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
7	Subnet_Mask	Subnet mask for ip Aliasing	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

12.20 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

12.21 net ipv6_tunnel isatap add

S.No	Command Name	Description	Type and Description
1	save	Save isatap tunnel configuration changes.	
2	exit	Save isaptap 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 w ith this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 netw ork), 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 w here each part is in the range 0-255

12.22 net ipv6_tunnel isatap edit <Itrow_id>

S.No	Command Name	Description	Type and Description
1	*<Itrow_id>*	isatap Tunnel configuration mode.	Unsigned integer
2	save	Save isatap tunnel configuration changes.	
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 w ith this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 netw ork), 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

12.23 net ipv6_tunnel isatap delete <ltrow_id>

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

12.24 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 Classical Routing mode.	routing mode type

12.25 net Option Option1 ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv4 Option configuration changes.	
2	cancel	Roll back ipv4 Option configuration changes.	
3	exit	Save ipv4 Option configuration changes and current mode.	
4	isp_connection_type	Select among the options: STATIC, DHCP Client, PPPoE, PPTP, L2TP, Russian PPTP, Russian L2TP, Japanese Multiple 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 address, fill this fields with Static IP address assigned to you. This will identify the router to your ISP.	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 ISPb 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. 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
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
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
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
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	
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 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 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 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
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

12.26 net Option Option2 ipv4 configure

S.No	Command Name	Description	Type and Description

1	save	Save ipv4 Option configuration changes.	
2	cancel	Roll back ipv4 Option configuration changes.	
3	exit	Save ipv4 Option configuration changes and current mode.	
4	isp_connection_type	Select among the options: STATIC, DHCP Client, PPPoE, PPTP, L2TP, Russian PPTP, Russian L2TP, Japanese Multiple PPPoE	OPTION2 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 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 ISPb 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. 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
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 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
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
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
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. 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 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 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 static IP address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise	Boolean choice

		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

12.27 net Option mode configure

S.No	Command Name	Description	Type and Description
1	save	Save Option mode configuration changes.	
2	cancel	Roll back ipv4 Option configuration changes.	
3	exit	Save Option mode configuration changes and current mode.	
4	Option_mode_type	Select among the options: SINGLE_OPTION, LOAD_BALANCING, AUTO_ROLLOVER	Types of OPTION modes
5	loadbalancing	If Mode Type selected is LOAD_BALANCING, this field gives you options to configure LOAD_BALANCING credentials	
6	loadbalancing algo	Enter the type of LoadBalancing Algo	Types of Loadbalancing algorithms
7	loadbalancing failover_method	Select the Fail Over detection method	
8	loadbalancing spillover	Spill Over Configuration Parameters	
9	loadbalancing spillover load_tolerance	Percentage of max bandwidth after which the router switches to secondary OPTION	Unsigned integer
10	loadbalancing spillover max_bandwidth	Sets the maximum bandwidth tolerable by the Primary OPTION.If the bandwidth goes below the load tolerance value of configured Max Bandwidth, the router switches to secondary OPTION.	Unsigned integer
11	loadbalancing failover_method type	Select the Fail Over detection method	Types of Faillover Detection methods
12	loadbalancing failover_method dns		
13	loadbalancing failover_method dns ipaddr_Option1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

14	loadbalancing failover_method dns ipaddr_Option2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
15	loadbalancing failover_method ping		
16	loadbalancing failover_method ping ipaddr_Option1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
17	loadbalancing failover_method ping ipaddr_Option2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
18	loadbalancing failover_method retry_interval		idle timeout value type.
19	loadbalancing failover_method retry_attempts		number in range of 2 to 999
20	rollover	Option Mode in Auto Rollover	
21	rollover Option_port	Select the Auto rollover Option port	OPTION interface type
22	rollover Option_port_Sec	Select the Auto rollover Option port	OPTION interface type
23	rollover failover_method	Select the Fail Over detection method	
24	rollover failover_method type	Select the Fail Over detection method	Types of Faillover Detection methods
25	rollover failover_method dns		
26	rollover failover_method dns ipaddr_Option1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
27	rollover failover_method dns ipaddr_Option2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
28	rollover failover_method ping		
29	rollover failover_method ping ipaddr_Option1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
30	rollover failover_method ping ipaddr_Option2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
31	rollover failover_method retry_interval		idle timeout value type.
32	rollover failover_method retry_attempts		number in range of 2 to 999
33	singleport		
34	singleport Option_port		OPTION interface type

12.28 net Option port_setup configure

S.No	Command Name	Description	Type and Description
1	save	Save Option port settings.	

2	exit	Save Option port settings and exit current mode.	
3	cancel	Roll back Option port settings changes.	
4	respond_ping	Disable or Enable ping on Option side	Boolean choice
5	Option1	Option1 port settings	
6	Option1 mtu_type	Enter MTU type	mtu type
7	Option1 mtu_size	Enter MTU size for Option1	mtu size
8	Option port_speed	Enter the type of port speed for Option1	Port Speed types
9	Option2	Option2 port settings	
10	Option2 mtu_type	Enter MTU type	mtu type
11	Option2 mtu_size	Enter MTU size for Option2	mtu size
12	Option2 port_speed	Enter the type of port speed for Option2	Port Speed types

12.29 net Option configurable_port configure

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

12.30 net Option Option1 ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv6 Option1 configuration changes.	
2	cancel	Roll back ipv6 Option configuration changes.	
3	exit	Save ipv6 Option1 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 w here each part is in the range [0-9A-Fa-f:]
10	static prefix	set prefix length	Unsigned integer
11	static gatew ay_address	Set ipv6 gatew ay address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here 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 w here 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 w here 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 passw ord 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.	OPTION interface type
19	pppoe primary_dns	Valid primary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here 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 w here each part is in the range [0-9A-Fa-f:]

12.31 net Optionn Option2 ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv6 Option2 configuration changes.	
2	cancel	Roll back ipv6 Option2 configuration changes.	
3	exit	Save ipv6 Option2 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 w here each part is in the range [0-9A-Fa-f:]
10	static prefix	set prefix length	Unsigned integer
11	static gatew ay_address	Set ipv6 gatew ay address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here 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:a

			bcd: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.	OPTION 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:]

12.32 net routing ospfv2 configure *<ltinterface>*

S.No	Command Name	Description	Type and Description
1	*<ltinterface>*	ospfv2 configuration mode.	
2	save	Save OSPFv2 configuration changes.	
3	exit	Save OSPFv2 configuration changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	enable	Enable/Disable OSPFv2 for a particular interface.	Boolean choice
6	area	Give the area to which the interface belongs	Unsigned integer
7	priority	Helps to determine the OSPFv2 designated router for a network.The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0, makes the router ineligible to be come Designated Router. The default value is 1.	Unsigned integer
8	hello_interval	The number of seconds for HelloInterval timer value.Setting this value, Hello packet will be sent every timer value seconds on the specified interface. This value must be the same for all routers attached to a common network. The default value is 10 seconds.	Unsigned integer
9	dead_interval	The number of seconds that a deviceb s hello packets must not have been seen before its neighbors declare the OSPF router down.This value must be the same for all routers attached to a common network.The default value is 40 seconds.	Unsigned integer
10	cost	The cost of sending a packet on an OSPFv2 interface	Unsigned integer
11	auth_type	Give the authentication type used for OSPFv2.If Authentication type is none the interface does not authenticate ospf packets.If Authentication Type is	OSPF Authentication type

		Simple then ospf packets are authenticated using simple text key.If Authentication Type is MD5 then the interface authenticates ospf packets with MD5 authentication.	
12	auth_key	Text Key for Simple Authentication type	String
13	md5_key_id	Give MD5 Key id	Unsigned integer
14	md5_auth_key	Give MD5 text key	String

12.33 net routing ospfv3 configure <ltinterface>

S.No	Command Name	Description	Type and Description
1	*<ltinterface>*	ospfv3 configuration mode.	
2	save	Save OSPFv3 configuration changes.	
3	exit	Save OSPFv3 configuration changes and exit current mode.	
4	cancel	Roll back configuration changes.	
5	enable	Enable/Disable OSPFv3 for a particular interface.	Boolean choice
6	priority	Helps to determine the OSPFv3 designated router for a network.The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0, makes the router ineligible to become Designated Router. The default value is 1.	Unsigned integer
7	hello_interval	The number of seconds for HelloInterval timer value.Setting this value, Hello packet will be sent every timer value seconds on the specified interface. This value must be the same for all routers attached to a common network. The default value is 10 seconds.	Unsigned integer
8	dead_interval	The number of seconds that a deviceb s hello packets must not have been seen before its neighbors declare the OSPF router down.This value must be the same for all routers attached to a common network.The default value is 40 seconds.	Unsigned integer
9	cost	The cost of sending a packet on an OSPFv3 interface	Unsigned integer

12.34 net port management configure <ltportName>

S.No	Command Name	Description	Type and Description
1	*<ltportName>*	port management configuration mode.	Port name
2	save	Save port management configuration changes.	
3	exit	Save port management configuration changes and exit current mode.	
4	cancel	Roll back port management configuration changes.	
5	enable	Enable/Disable the port status	Boolean choice
6	auto_negotiation_enable	Select this to let the gateway and network to determine the optimal port settings.	Boolean choice
7	duplex_mode	Choose between Half Duplex and Full Duplex based on the port support. The default is Full Duplex for all ports.	select the duplex mode
8	speed	One of three port speeds can be selected: 10 Mbps, 100 Mbps and 1000 Mbps (i.e. 1 Gbps). The default setting is 1000 Mbps for all ports	select the speed

12.35 net Option pppoe configure

S.No	Command Name	Description	Type and Description
1	save	Save pppoe configuration changes.	
2	cancel	Roll back pppoe configuration changes.	
3	exit	Save pppoe configuration changes and current mode.	
4	UserName	Set user name	String
5	Password	Set Password	String
6	AuthMode	Select Authentication Type	PPPOE Authentication Types.
7	Service	Set service name	String
8	CompressionEnable	Enable/Disable Compression Negotiation	Boolean choice
9	ConnectionMode	Set Connection Mode type	Boolean choice
10	IdleTimeOutValue	Set Idle TimeOut Value (in min)	PPPOE idle timeout Type.
11	GetIpFromIspEnable	Enable/Disable GetIpFromIsp	Boolean choice
12	StaticIp	Set static IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	NetMask	Set subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	GetDnsFromIspEnable	Enable/Disable GetDnsFromIsp	Boolean choice
15	PrimaryDns	Set Primary DNS	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
16	SecondaryDns	Set Secondary DNS	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12.36 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	OPTION 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 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

12.37 net routing protocol_binding edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	OPTION 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

12.38 net routing protocol_binding enable <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	OPTION 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

12.39 net routing protocol_binding disable <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	OPTION 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

12.40 net routing protocol_binding delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	OPTION 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

12.41 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 (RAbs) to all interfaces else Y	radvd advertizement mode type
6	interval	The time in seconds between sending unsolicited multicast RAbs. The default is 30 seconds.	PPPOE idle timeout Type.
7	flags	RA Flags	
8	flags managed_enable	Chose Managed to use the administered /stateful protocol for 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 routerbs RADVD process	radvd preference type
11	mtu	This is used in RAbs to ensure all nodes on the network use the same MTU value in the cases where the LAN MTU is not well known. The	mtu size

		default is 1500	
12	life_time	The lifetime in seconds of the route. The default is 3600 seconds.	Unsigned integer

12.42 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 w hether 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 w hich the advertisements are sent	Unsigned integer
6	prefix_address	It specifies the IPv6 netw ork 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 netw ork portion of the address	Unsigned integer
8	prefix_life_time	The length of time over w hich the requesting router is allow ed to use the prefix	Unsigned integer

12.43 net radvd pool edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	radvd Pool configuration mode.	Unsigned integer
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 w hether 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 w hich the advertisements are sent	Unsigned integer
7	prefix_address	It specifies the IPv6 netw ork 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 netw ork portion of the address	Unsigned integer
9	prefix_life_time	The length of time over w hich the requesting router is allow ed to use the prefix	Unsigned integer

12.44 net radvd pool delete <ltrow_id>

S.No	CommandName	Description	Type and Description
1	*<ltrow_id>*	radvd pool configuration mode.	Unsigned integer

12.45 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.	
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
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
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)

12.46 net routing static ipv4 configure <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	Add new static routes.	String
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	interface	Set the interface for which the rule applies.	OPTION interface type
9	metric	Set the metric for this route.	Unsigned integer
10	private_flag	Defines whether the route can be shared with other gateways when RIP is enabled	Boolean choice
11	active_flag	Defines whether its an active route	Boolean choice

12.47 net routing static ipv6 configure <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	Add new IPV6 static routes.	String
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 w here each part is in the range [0-9A-Fa-f:]
6	prefix	Set the prefix length for this rule.	Unsigned integer
7	gatew ay_address	Set the gatew ay IPV6.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here 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 w hether its an active IPV6 route	Boolean choice

12.48 net routing static ipv4 delete <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	Delete a specific route.	String

12.49 net routing static ipv6 delete <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	Delete a specific IPV6 route.	String

12.50 net tahi add-default-route <ltip_address>

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

12.51 net tahi add-route <ltip_address> <ltgw>

S.No	Command Name	Description	Type and Description
1	*<ltip_address> <ltgw>*	add ipv6 route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:] IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.52 net tahi del-route <ltip_address> <ltgw>

S.No	Command Name	Description	Type and Description
1	*<ltip_address> <ltgw>*	add ipv6 route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:] IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.53 net tahi ipv6-Alias-Add(LAN) <ltip6_address>

S.No	Command Name	Description	Type and Description
1	*<ltip6_address>*	Add ipv6 address to LAN interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.54 net tahi ipv6-Alias-Del(LAN) <ltip6_address>

S.No	Command Name	Description	Type and Description
1	*<ltip6_address>*	Delete an ipv6 address from LAN interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.55 net tahi ipv6-Alias-Add(OPTION) <ltip6_address>

S.No	Command Name	Description	Type and Description
1	*<ltip6_address>*	Add ipv6 address to OPTION interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.56 net tahi ipv6-Alias-Del(OPTION) <ltip6_address>

S.No	Command Name	Description	Type and Description
1	*<ltip6_address>*	Delete an ipv6 address from OPTION interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.57 net tahi reachable-time <lttime>

S.No	Command Name	Description	Type and Description

1	*<lttime>*	set the reachable time of neighbour cache entries	number in range of 30 to 150

12.58 net tahi ping6 <ltip> <ltsize>

S.No	Command Name	Description	Type and Description
1	*<ltip> <ltsize>*	ping6 on LAN interface with count one	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:] number in range of 1 to 1500

12.59 net tahi pmtu-route-add <ltipAdd>

S.No	Command Name	Description	Type and Description
1	*<ltipAdd>*	add ipv6 route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

12.60 net upnp configure

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

Chapter 13. Configuration commands VPN

13.1 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.	
3	exit	Save l2tp server configuration changes and exit current mode.	
4	enable	enable/disable L2TP server.	Boolean choice
5	start_address	L2TP server starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	end_address	L2TP server ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	EnablePap	enable pap authentication	Boolean choice
8	EnableChap	enable chap authentication	Boolean choice
9	EnableMSChapChap	enable MSchap authentication	Boolean choice
10	MSChapv2Enable	enable MSChapv2Enable authentication	Boolean choice
11	l2tpSecretKeyEnable	L2TP Enanle secret key	Boolean choice
12	secretKey	L2TP secret Key	String

13.2 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	Unsigned integer
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

13.3 vpn pptp client_action <ltaction>

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

13.4 vpn pptp server configure

S.No	Command Name	Description	Type and Description
1	save	Save pptp server configuration changes.	
2	cancel	Roll back pptp server configuration changes.	
3	exit	Save pptp server configuration changes and exit current mode.	
4	enable	enable/disable PPTP server.	Boolean choice
5	Natenable	enable/disable PPTP NAT routing mode	Boolean choice
6	start_address	PPTP server starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	end_address	PPTP server ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	pap_enable	PPTP server PAP authentication	Boolean choice
9	chap_enable	PPTP server CHAP authentication	Boolean choice
10	mschap_enable	PPTP server MSCHAP authentication	Boolean choice
11	mschapv2_enable	PPTP server MSCHAPV2 authentication	Boolean choice
12	Mppe40Enable	PPTP server Mppe40	Boolean choice
13	Mppe128Enable	PPTP server Mppe128	Boolean choice
14	MppeStatefullEnable	PPTP server MppeStatefull	Boolean choice
15	UserTimeOut	PPTP server User TimeOut	Boolean choice

13.5 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 128 characters and no ' or empty space or "

5	portal_title	Specify the portal title	String, Max 128 characters and no ' or empty space or "
6	banner_title	Specify the banner title	String, Max 128 characters and no ' or empty space or "
7	banner_message	Specify the banner message	String, No ' or empty space or "
8	display_banner	Specify whether the banner message should be displayed	Boolean choice
9	enable_httpmetatags	Specify whether the http meta tags should be enabled	Boolean choice
10	enable_activexwebcachecleaner	Specify whether the activex webcache cleaner should be enabled	Boolean choice
11	enable_vpntunnel	Specify whether the vpn tunnel should be enabled	Boolean choice
12	enable_portforwarding	Specify whether the port forwarding should be enabled	Boolean choice

13.6 vpn sslvpn portal-layouts edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	portal_name	Specify the portal name	String, Max 128 characters and no ' or empty space or "
6	portal_title	Specify the portal title	String, Max 128 characters and no ' or empty space or "
7	banner_title	Specify the banner title	String, Max 128 characters and no ' or empty space or "
8	banner_message	Specify the banner message	String, No ' or empty space or "
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_activexwebcachecleaner	Specify whether the activex webcache 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

13.7 vpn sslvpn portal-layouts delete <ltrow_id>

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

13.8 vpn sslvpn portal-layouts set-default <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Set the portal as default	Unsigned integer

13.9 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

13.10 vpn sslvpn portforwarding appconfig delete <ltrow_id>

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

13.11 vpn sslvpn portforwarding hostconfig add

S.No	Command Name	Description	Type and Description
1	save	Save portforwarding Host settings	
2	exit	Save 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 "

13.12 vpn sslvpn portforwarding hostconfig delete <ltrow_id>

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

13.13 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 and no ' or empty space or "
5	service_type	service type	sslvpn resource

13.14 vpn sslvpn resource configure add <ltresource_name>

S.No	Command Name	Description	Type and Description
1	*<ltresource_name>*	Add an sslvpn resource object	String, Max 128 characters and no ' or empty space or "
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	resource_name	resource name	String, Max 128 characters and no ' or empty space or "
6	object_type	object type	sslvpn resource object type
7	object_address	object address	IP address A.A.A.BBB.CCC.DDD w here each part is in the range 0-255
8	mask_length	mask length	number in range of 1 to 32
9	start_port	start port	Port number
10	end_port	end port	Port number
11	icmp_block	block icmp	source address type for users ip policy

13.15 vpn sslvpn resource configure delete <ltrow_id>

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

13.16 vpn sslvpn resource delete <ltrow_id>

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

13.17 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, Max 128 characters and no ' or empty space or "
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 and no ' or empty space or "
14	policy_permission	policy permission	sslvpn policy type
15	icmp_block	block icmp	source address type for users ip policy

13.18 vpn sslvpn policy edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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_type	policy type	sslvpn policy type
6	policy_owner	policy owner	String
7	destination_objecttype	destination object type	sslvpn policy destination type
8	policy_name	policy name	String, Max 128 characters and no ' or empty space or "
9	policy_address	policy address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	policy_masklength	policy masklength	number in range of 1 to 32
11	start_port	start port	

			Port number
12	end_port	end port	Port number
13	service_type	service type	sslvpn resource
14	resource_name	resource name	String, Max 128 characters and no ' or empty space or "
15	policy_permission	policy permission	sslvpn policy type
16	icmp_block	block icmp	source address type for users ip policy

13.19 vpn sslvpn policy delete <ltrow_id>

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

13.20 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 w here each part is in the range 0-255
7	secondary_dns	secondary dns server	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
8	begin_clientaddress	Client Address Range Begin	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
9	end_clientaddress	Client Address Range End	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
10	lcp_timeout	lcp timeout	Unsigned integer

13.21 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 netw ork	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
5	subnet_mask	subnet mask	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

13.22 vpn sslvpn route delete <ltrow_id>

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

13.23 vpn sslvpn users domains add

S.No	Command Name	Description	Type and Description
1	save	Save users domains configuration changes.	
2	exit	Save users domains configuration changes and exit current mode.	
3	cancel	Roll back users domains configuration changes.	
4	domain_name	Specify the domain name	String
5	authentication_type	Specify the authentication type	Users domain authentication type
6	portal	Select the portal	String
7	authentication_server 1	Specify the authentication server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	authentication_server 2	Specify the authentication server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	authentication_server 3	Specify the authentication server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	timeout	Specify the timeout value	Unsigned integer
11	retries	Specify the max retries	Unsigned integer
12	authentication_secret	Enter the secret key	String
13	authentication_secret 2	Enter the secret key	String
14	workgroup	Specify the work group	String
15	second_workgroup	Specify the work group	String
16	ldap_base_dn	Specify the ldap base domain name	String
17	second_ldap_base_d n	Specify the ldap base domain name	String
18	active_directory_dom ain	Specify the active directory domain	String
19	second_active_direct ory_domain	Specify the active directory domain	String

13.24 vpn sslvpn users domains edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users domain configuration mode	Unsigned integer

2	save	Save users domains configuration changes.	
3	exit	Save users domains configuration changes and exit current mode.	
4	cancel	Roll back users domains configuration changes.	
5	domain_name	Specify the domain name	String
6	authentication_type	Specify the authentication type	Users domain authentication type
7	portal	Select the portal	String
8	authentication_server1	Specify the authentication server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	authentication_server2	Specify the authentication server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	authentication_server3	Specify the authentication server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	timeout	Specify the timeout value	Unsigned integer
12	retries	Specify the max retries	Unsigned integer
13	authentication_secret	Enter the secret key	String
14	authentication_secret2	Enter the secret key	String
15	workgroup	Specify the work group	String
16	second_workgroup	Specify the work group	String
17	ldap_base_dn	Specify the ldap base domain name	String
18	second_ldap_base_dn	Specify the ldap base domain name	String
19	active_directory_domain	Specify the active directory domain	String
20	second_active_directory_domain	Specify the active directory domain	String

13.25 vpn sslvpn users domains delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users domain delete mode	Unsigned integer

13.26 vpn sslvpn users groups add

S.No	Command Name	Description	Type and Description
1	save	Save users groups configuration changes.	
2	exit	Save users groups configuration changes and exit current mode.	
3	cancel	Roll back users groups configuration changes.	
4	group_name	Specify the group name	String

5	domain_name	Specify the domain name for the group	String
6	idle_timeout	Specify the idle timeout for the group	idle timeout value for user.

13.27 vpn sslvpn users groups edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users groups configuration mode	Unsigned integer
2	save	Save users groups configuration changes.	
3	exit	Save users groups configuration changes and exit current mode.	
4	cancel	Roll back users groups configuration changes.	
5	group_name	Specify the group name	String
6	domain_name	Specify the domain name for the group	String
7	idle_timeout	Specify the idle timeout for the group	idle timeout value for user.

13.28 vpn sslvpn users groups delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users group delete mode	Unsigned integer

13.29 vpn sslvpn users users add

S.No	Command Name	Description	Type and Description
1	save	Save users configuration changes.	
2	exit	Save users configuration changes and exit current mode.	
3	cancel	Roll back users configuration changes.	
4	user_name	Specify the user name	String
5	first_name	Specify the user's first name	String
6	last_name	Specify the user's last name	String
7	user_type	Specify the user type	Users type
8	group	Specify the user's group	String
9	password	Specify the user's password	String
10	confirm_password	confirmthe user's password	String
11	idle_timeout	Enter the user's timeout value	idle timeout value for user.

13.30 vpn sslvpn users users edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users configuration mode	Unsigned integer
2	save	Save users configuration changes.	
3	exit	Save users configuration changes and exit current mode.	
4	cancel	Roll back users configuration changes.	
5	user_name	Specify the user name	String
6	first_name	Specify the user's first name	String
7	last_name	Specify the user's last name	String
8	user_type	Specify the user type	Users type
9	group	Specify the user's group	String
10	password	Specify the user's password	String
11	confirm_password	confirmthe user's password	String
12	idle_timeout	Enter the user's timeout value	idle timeout value for user.

13.31 vpn sslvpn users users login_policies <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users login policy configuration mode	Unsigned integer
2	save	Save users login policy configuration changes.	
3	exit	Save users login policy configuration changes and exit current mode.	
4	cancel	Roll back users login policy configuration changes.	
5	disable_login	enable/disable login	Boolean choice
6	deny_login_from_option_interface	enable/disable login from option	Boolean choice

13.32 vpn sslvpn users users browser_policies <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users browsers policy configuration mode	Unsigned integer
2	save	Save users browser policy configuration changes.	
3	exit	Save users browser policy configuration changes and exit current mode.	
4	cancel	Roll back users browser policy configuration changes.	
5	allow_login_from_defined_browsers	enable/disable login from defined browser	Boolean choice
6	add_client_browser	add defined browser	

			Boolean choice
7	client_browser	add defined browser	Supported browsers
8	del_client_browser	delete defined browser	Boolean choice

13.33 vpn sslvpn users users ip_policies configure <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users ip policy configuration mode	Unsigned integer
2	save	Save users ip policy configuration changes.	
3	exit	Save users ip policy configuration changes and exit current mode.	
4	cancel	Roll back users ip policy configuration changes.	
5	allow_login_from_defined_addresses	enable/disable login from defined addresses	Boolean choice
6	add_ip_address	add ip address	Boolean choice
7	source_address_type	Set the source address type	source address type for users ip policy
8	source_address	Set the source address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	mask_length	Set the source network mask length	number in range of 1 to 32

13.34 vpn sslvpn users users ip_policies delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users ip policy delete mode	Unsigned integer

13.35 vpn sslvpn users users delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Users delete mode	Unsigned integer

13.36 vpn ipsec policy configure <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	vpn policy configuration mode	String
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
6	general_ike_version	Setting version ikev1 or ikev2	IPsec VPN IKE Version
7	general_ip_protocol_version	Setting protocol version ipv5 or ipv6	
8	general_ipsec_mode	Setting ipsec mode for the vpn policy	VPN ipsec modes
9	general_select_local_gateway	Setting local gateway for the vpn policy	VPN gateway
10	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
11	general_remote_end_point	The IP address or Internet Name/FQDN of the remote gateway or client PC.	
12	general_remote_end_point ip_address	The IP address of the remote gateway or client PC.	
13	general_remote_end_point fqdn	The IP address or Internet Name/FQDN of the remote gateway or client PC.	String
14	general_enable_mode_config	enable/disable mode config	Boolean choice
15	general_enable_netbios	enable/disable this to allow NetBIOS broadcasts to travel over the VPN tunnel.	Boolean choice
16	general_enable_rollover	enable/disable rollover	Boolean choice
17	general_protocol	Setting protocol esp or ah	IPsec VPN Protocol
18	general_enable_dhcp	enable/disable dhcp.	Boolean choice
19	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
20	general_local_start_address	IP address from where the range needs to begin	
21	general_local_end_address	IP address where the range needs to end	
22	general_local_subnet_mask	Subnet mask of the subnet used	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
23	general_local_prefix_length	Prefix length of the ipv6 subnet used	IPv6 Prefix length
24	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
25	general_remote_start_address	IP address from where the range needs to begin	
26	general_remote_end_address	IP address where the range needs to end	
27	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
28	general_remote_prefix_length	Prefix length of the ipv6 subnet used	

			IPv6 Prefix length
29	general_enable_keepalive	enable/disable keepalive	Boolean choice
30	general_keepalive_sourceip	keepalive sourceip	
31	general_keepalive_destinationip	keepalive destinationip	
32	general_keepalive_detection_period	keepalive detection period	
33	general_keepalive_failure_count	keepalive failure count	
34	manual_spi_in	Takes a hexadecimal value betw een 3 and 8 characters.	Takes a hexadecimal value betw een 3 and 8 characters
35	manual_spi_out	Takes a hexadecimal value betw een 3 and 8 characters.	Takes a hexadecimal value betw een 3 and 8 characters
36	manual_encryption_algorithm	The algorithm used to encrypt the data	vpn encryption algorithm
37	manual_key_length	The key length for the algorithm.	Unsigned integer
38	manual_encryption_key_in	Encryption key of the inbound policy. The length of the key depends on the algorithm chosen	String
39	manual_encryption_key_out	Encryption key of the outbound policy. The length of the key depends on the algorithm chosen.	String
40	manual_authentication_algorithm	Algorithm used to verify the integrity of the data.	vpn authentication algorithm
41	manual_authentication_key_in	This is the integrity key (for ESP w ith Integrity-mode) for the inbound policy and depends on the algorithm chosen	String
42	manual_authentication_key_out	This is the integrity key (for ESP w ith Integrity-mode) for the outbound policy and depends on the algorithm chosen	String
43	auto_phase1_exchange_mode	Setting IKE exchange Mode	VPN Exchange Mode
44	auto_phase1_enable_nat_traversal	Enabling/Disabling Nat traversal	Boolean choice
45	auto_phase1_nat_keepalive_frequecy	Setting IKE nat alive frequency	Unsigned integer
46	auto_phase1_local_identtype	Setting IKE local identifier type	IPsec VPN IKE local identifier type
47	auto_phase1_direction_type	Setting IKE direction type	IPsec VPN IKE direction Mode
48	auto_phase1_local_identifier	Setting IKE local identifier	String
49	auto_phase1_remote_identtype	Setting IKE remote identifier	IPsec VPN IKE local identifier type
50	auto_phase1_remote_identifier	Setting IKE remote identifier	String
51	auto_phase1_encryption_algorithm	Setting IKE encryption algorithm	IPsec VPN IKE encryption algorithm type
52	auto_phase1_key_length	The key length for the algorithm.	Unsigned integer
53	auto_phase1_auth_algorithm	Setting IKE authentication algorithm	IPsec VPN IKE authentication algorithm type
54	auto_phase1_auth_method	Setting IKE authentication algorithm method	IPsec VPN IKE authentication algorithm method
55	auto_phase1_dh_group	Setting IKE Diffie-Hellman (DH)	

		Group	IPsec VPN IKE Diffie-Hellman (DH) Group type
56	auto_phase1_sa_lifetime	Setting IKE SA lifetime in seconds	Unsigned integer
57	auto_phase1_pre_shared_key	Setting IKE pre shared key	String
58	auto_phase1_enable_dead_peer_detection	Enabling/Disabling dead peer detection	Boolean choice
59	auto_phase1_detection_period	Setting dead peer detection time period	Unsigned integer
60	auto_phase1_reconnect_failure_count	Setting dead peer detection failure count	Unsigned integer
61	auto_phase1_extended_authentication	setting extended authentication method	IPsec VPN IKE extended authentication method
62	auto_phase1_authentication_type	setting extended authentication type	IPsec VPN IKE extended authentication method
63	auto_phase1_xauth_username	Username for extended authentication	String
64	auto_phase1_xauth_password	Password for extended authentication	String
65	auto_phase2_sa_lifetime	vpn auto policy phase2 configure	
66	auto_phase2_sa_lifetime seconds	Setting IKE SA lifetime in seconds	Unsigned integer
67	auto_phase2_sa_lifetime bytes	Setting IKE SA lifetime in bytes	Unsigned integer
68	auto_phase2_encryption_algorithm	The algorithm used to encrypt the data	vpn encryption algorithm
69	auto_phase2_key_length	The key length for the algorithm.	Unsigned integer
70	auto_phase2_authentication_algorithm	Algorithm used to verify the integrity of the data.	vpn authentication algorithm
71	auto_phase2_enable_pfskeygroup	Enable/Dlsable PFS key group	Boolean choice
72	auto_phase2_dh_group	Setting IKE Diffie-Hellman (DH) Group	IPsec VPN IKE Diffie-Hellman (DH) Group type

13.37 vpn ipsec policy enable <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	enable a vpn policy	String

13.38 vpn ipsec policy disable <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	disable a vpn policy	String

13.39 vpn ipsec policy delete <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	delete a vpn policy	String

13.40 vpn ipsec policy connect <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	connect a vpn tunnel	String

13.41 vpn ipsec policy drop <ltname>

S.No	Command Name	Description	Type and Description
1	*<ltname>*	drop a vpn tunnel	String

Chapter 14. Configuration commands Security

14.1 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 OPTION port.	Boolean choice
6	block_udp_flood	Enable or Disable UDP Flood on LAN port.	Boolean choice
7	block_icmp_notification	Enable or Disable ICMP notifications on Internet Ports.	Boolean choice
8	block_fragmented_packets	Enable or Disable Fragmented Packets on Internet Ports.	Boolean choice
9	block_multicast_packets	Enable or Disable Multicast packets on Internet Ports.	Boolean choice
10	synflood_dectect_rate	Configure the Syn flood Detect Rate	range of packets sent per second in dos attack types.
11	echostorm_flood_rate	Configure the Echo Storm Flood Rate	range of packets sent per second in dos attack types.
12	icmp_flood_rate	Configure the ICMP flood Rate	range of packets sent per second in dos attack types.

14.2 security advanced_network igmp setup

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

14.3 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
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

14.4 security application_rules edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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

14.5 security application_rules delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	application rules rules configuration mode.	Unsigned integer

14.6 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	start_port	port number of the Destination user	Port number
7	icmp_type	port number of the Destination user	number in range of 0-40(icmp) or 1-255(icmpv6)
8	finish_port	Port of the Destiation user	Port number

14.7 security firewall custom_service edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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.	
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	start_port	port number of the Destination user	Port number
8	icmp_type	port number of the Destination user	number in range of 0-40(icmp) or 1-255(icmpv6)
9	finish_port	Port of the Destiation user	Port number

14.8 security firewall custom_service delete <ltrow_id>

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

14.9 security firewall ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save Firew all IPV4 rules configuration changes.	
2	exit	Save Firew all IPV4 rules configuration changes and exit current mode.	
3	cancel	Roll back IPV4 rules configuration changes.	
4	from_zone	Set from Zone security type	firew all 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
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 Destiation 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	option_interface	OPTION interface for Source NAT settings	OPTION interface type
23	snat_address	IP of the SNAT Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
24	dnat_port	The port number to use for DNAT, required if port forwarding is enabled	Port number
25	port_forwarding_enable	enable/disable port forwarding based on this firewall rule configuration settings	Boolean choice
26	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
27	dnat_ipaddress	Set it as Dedicated/configured OPION	OPTION interface type

14.10 security firewall ipv4 default_outbound_policy <ltdefault_outbound_policy>

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

14.11 security firewall ipv4 edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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 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 Destiation 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	option_interface	OPTION interface for Source NAT settings	OPTION interface type
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	Set it as Dedicated/configured OPION	OPTION interface type

14.12 security firewall ipv4 enable <ltrow_id>

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

14.13 security firewall ipv4 disable <ltrow_id>

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

14.14 security firewall ipv4 delete <ltrow_id>

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

14.15 security firewall ipv4 move <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Firewall IPV4 Rule reordering mode.	Row id(s) a,b,c where each part is a valid row id 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

14.16 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	PPTP	Protocal to be enabled at ALGs	

			Boolean choice
5	Ipsec	Protocal to be enabled at ALGs	Boolean choice
6	Rtsp	Protocal to be enabled at ALGs	Boolean choice
7	Sip	Protocal to be enabled at ALGs	Boolean choice
8	H323	Protocal to be enabled at ALGs	Boolean choice
9	Smtp	Protocal to be enabled at ALGs	Boolean choice
10	Dns	Protocal to be enabled at ALGs	Boolean choice
11	Tftp	Protocal to be enabled at ALGs	Boolean choice

14.17 security firewall ipv6 edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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:abcd 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:abcd 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:abcd:abcd where each part is in the range [0-9A-Fa-f:]
18	destination_end_address	IP of the Destiation user	IP address

			abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]
19	destination_address_prefix	Prefix Length of the Destination user	String

14.18 security firewall ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Save Firew all IPV6 rules configuration changes.	
2	exit	Save Firew all 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	firew all 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	firew all rule action type
9	schedule	Schedule for w hich the rule is applicable	String
10	source_address_type	Type of the source user	firew all rule address type
11	destination_address_type	Type of the destination user	firew all rule address type
12	log	Log Alw ays or Never	firew all rule log enable/disable
13	source_start_address	IP of the Source user	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here 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:abcd w here 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:abcd w here each part is in the range [0-9A-Fa-f:]
17	destination_end_address	IP of the Destiation user	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]
18	destination_address_prefix	Prefix Length of the Destination user	String

14.19 security firewall ipv6 enable <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Firew all IPV6 rules configuration mode.	Unsigned integer

14.20 security firewall ipv6 disable <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Firew all IPV6 Rules configuration mode.	Unsigned integer

14.21 security firewall ipv6 delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Firew all IPV6 Rules configuration mode.	Unsigned integer

14.22 security firewall ipv6 move <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	Firew all IPV6 Rule reordering mode.	Row id(s) a,b,c w here each part is a valid row id in the range [0-9]
2	save	Save Firew all IPV6 rule reordering changes.	
3	exit	Save Firew all 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

14.23 security firewall ipv6 default_outbound_policy <ltdefault_outbound_policy>

S.No	Command Name	Description	Type and Description
1	*<ltdefault_outbound_policy>*	Firew all Settings, IPv6 Default Outbound Policy configuration mode.	Boolean choice

14.24 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

14.25 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
9	tcp_session_cleanup_latency	TCP Session Cleanup Latency	Unsigned integer

14.26 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	String
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)
22	time_of_day end hours	hours	schedule time unit type.
23	time_of_day end meridiem	meridiem	Schedule Meridiem Types.

14.27 security schedules edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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 w hich a rule is to be added	String
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 w ednesday	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.
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.

14.28 security schedules delete <ltrow_id>

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

14.29 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	Set the mac address policy	policy type for mac addresses

14.30 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 policies will be applied	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

14.31 security mac_filter source edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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

14.32 security mac_filter source delete <ltrow_id>

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

14.33 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	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 w here each part is in the range 0-255
7	log_dropped_packets	Specify logging option for this rule	Boolean choice

14.34 security ip_or_mac_binding edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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	name	Specify a unique name for this rule.	String
6	mac_address	enter mac address to w hich policies w ill be applied	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
7	ip_address	enter ip address to w hich policies will be applied	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
8	log_dropped_packets	Specify logging option for this rule	Boolean choice

14.35 security ip_or_mac_binding delete <ltrow_id>

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

14.36 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
5	pptp_enable	Enable or Disable PPTP Passthrough.	Boolean choice
6	l2tp_enable	Enable or Disable L2TP Passthrough.	Boolean choice

14.37 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

14.38 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

14.39 security website_filter approved_urls edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_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

14.40 security website_filter approved_urls delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	trusted Domains configuration mode.	Unsigned integer

14.41 security website_filter blocked_keywords add

S.No	Command Name	Description	Type and Description
1	save	Save blocked keyw ords configuration changes.	
2	exit	Save blocked keyw ords configuration changes and exit current mode.	
3	cancel	Roll back blocked keyw ords configuration changes.	
4	blocked_keyw ord	enter keyw ord to be blocked	String

14.42 security website_filter blocked_keywords edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	blocked Keyw ords configuration mode.	Unsigned integer
2	save	Save blocked keyw ords configuration changes.	
3	exit	Save blocked keyw ords configuration changes and exit current mode.	
4	cancel	Roll back blocked keyw ords configuration changes.	
5	blocked_keyw ord	enter keyw ord to be blocked	String

14.43 security website_filter blocked_keywords delete <ltrow_id>

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

14.44 security website_filter blocked_keywords enable <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	blocked Keyw ords configuration mode.	Unsigned integer

14.45 security website_filter blocked_keywords disable <ltrow_id>

S.No	Command Name	Description	Type and Description
1	*<ltrow_id>*	blocked Keyw ords configuration mode.	Unsigned integer

Chapter 15. Configuration commands RADIUS

15.1 radius configure <*ltradius_server*>

S.No	Command Name	Description	Type and Description
1	*<ltradius_server>*	RADIUS configuration mode.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	save	Save RADIUS configuration changes.	
3	exit	Save RADIUS configuration changes and exit current mode.	
4	cancel	Roll back configuration changes	
5	radius-server	Set RADIUS server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	authentication-port	Set RADIUS server port.	Port number
7	secret	Set RADIUS server secret.	String
8	timeout	Set RADIUS server connection timeout.	Unsigned integer
9	retries	Set RADIUS server connection rety attempts.	Unsigned integer

15.2 radius delete <ltradius_server>

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

Chapter 16. Configuration commands HISTORY

16.1 history <*ltlimit*>

S.No	Command Name	Description	Type and Description
1	<*ltlimit*>	Display the current session's command line history	Unsigned integer

Chapter 17. Configuration commands License activate

17.1 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	

17.2 License activate *<ltactivationKey>*

S.No	Command Name	Description	Type and Description
1	<ltactivationKey>	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	