



UNIFIED SERVICES ROUTER CLI REFERENCE GUIDE

DSR-150 / 150N / 250 / 250N / 500 / 500N /
1000 / 1000N

RELEASE 1.05



SMALL BUSINESS GATEWAY SOLUTION

CLI Reference Guide

Unified Services Router

D-Link Corporation

Copyright © 2012.

<http://www.dlink.com>

CLI Reference Guide

DSR-150/150N/250/250N/500/500N/1000/1000N

Unified Services Router

Version 1.05

Copyright © 2012

Copyright Notice

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

Disclaimer

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

Limitations of Liability

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

Table of Contents

Chapter 1.	Introduction.....	8
1.1	Accessing the CLI.....	8
Chapter 2.	Basic commands available on the CLI.....	9
2.1	CONTEXT SENSITIVE HELP	9
2.2	AUTO-COMPLETION	9
2.3	MOVEMENT KEYS.....	9
2.4	DELETION KEYS	9
2.5	ESCAPE SEQUENCES	10
Chapter 3.	Command Hierarchy in CLI	11
3.1	CLI commands can be divided into 4 categories:	11
3.2	The router configuration is divided into 5 branches:	11
Chapter 4.	Global commands used in CLI	12
Chapter 5.	Show commands used in CLI	13
Chapter 6.	Utility commands used in CLI	18
6.1	util system_check ping <ltip_address>.....	18
6.2	util system_check dns_lookup <ltdns>.....	18
6.3	util system_check traceroute <ltip_address>.....	18
6.4	util system_check capturePackets start <ltinterface>.....	18
6.5	util system_check capturePackets download <ltfileName> <ltipAddr>.....	18
6.6	util cat <ltfileName>	19
6.7	util md5sum <ltfileName>	19
6.8	util copy <ltfileName1> <ltfileName2>	19
6.9	util usb_test <ltipAddr> <ltfileName>	19
Chapter 7.	Configure commands used in CLI	20
Chapter 8.	Configuration commands under branch NET	29
8.1	net bandwidth profile enable	29
8.2	net bandwidth profile add/edit.....	29
8.3	net bandwidth profile delete <row_id>	29
8.4	net bandwidth traffic_selector add	30
8.5	net bandwidth traffic_selector edit <ltrow_id>	30
8.6	net bandwidth traffic_selector delete <ltrow_id>	31
8.7	net ddns wan1 configure	31
8.8	net ddns wan2 configure	31
8.9	net lan dhcp reserved_ip configure <ltmac_address>.....	31
8.10	net lan dhcp reserved_ip delete <ltmac_address>	32
8.11	net wan dhcpc configure	32
8.12	net dmz configure	32

8.13	net dmz dhcp reserved_ip configure <ltmac_address>	33
8.14	net dmz dhcp reserved_ip delete <ltmac_address>	33
8.15	net ethernet configure <ltinterface_name>	34
8.16	net lan ipv4 configure	34
8.17	net lan ipv6 configure	36
8.18	net lan ipv6 pool configure <ltipv6PoolStartAddr>	36
8.19	net lan ipv6 pool delete <ltipv6PoolStartAddr>	37
8.20	net intel_Amt server configure	37
8.21	net intel_Amt_Reflector configure	37
8.22	net ip_Aliasing server add	38
8.23	net ip_Aliasing server edit <ltrow_id>	38
8.24	net ip_Aliasing server delete <ltrow_id>	38
8.25	net mode configure	39
8.26	net ipv6_tunnel isatap add	39
8.27	net ipv6_tunnel isatap edit <ltrow_id>	39
8.28	net ipv6_tunnel isatap delete <ltrow_id>	40
8.29	net routing mode configure	40
8.30	net wan wan1 ipv4 configure	40
8.31	net wan wan2 ipv4 configure	48
8.32	net wan wan3 threeG configure	56
8.33	net wan mode configure	57
8.34	net wan port_setup configure	59
8.35	net wan configurable_port configure	59
8.36	net wan wan1 ipv6 configure	59
8.37	net wan wan2 ipv6 configure	60
8.38	net routing ospfv2 configure <ltinterface>	61
8.39	net routing ospfv3 configure <ltinterface>	62
8.40	net port management configure <ltportName>	63
8.41	net wan pppoe configure	63
8.42	net routing protocol_binding add	64
8.43	net routing protocol_binding edit <ltrow_id>	64
8.44	net routing protocol_binding enable <ltrow_id>	65
8.45	net routing protocol_binding disable <ltrow_id>	66
8.46	net routing protocol_binding delete <ltrow_id>	66
8.47	net radvd configure	67
8.48	net radvd pool add	67
8.49	net radvd pool edit <ltrow_id>	68
8.50	net radvd pool delete <ltrow_id>	68
8.51	net routing dynamic configure	68
8.52	net routing static ipv4 configure <ltname>	70
8.53	net routing static ipv6 configure <ltname>	70
8.54	net routing static ipv4 delete <ltname>	71
8.55	net routing static ipv6 delete <ltname>	71

8.56	net tahi add-default-route <ltip_address>.....	71
8.57	net tahi add-route <ltip_address> <ltgw>.....	71
8.58	net tahi del-route <ltip_address> <ltgw>.....	72
8.59	net tahi ipv6-Alias-Add(LAN) <ltip6_address>.....	72
8.60	net tahi ipv6-Alias-Del(LAN) <ltip6_address>.....	72
8.61	net tahi ipv6-Alias-Add(WAN) <ltip6_address>.....	72
8.62	net tahi ipv6-Alias-Del(WAN) <ltip6_address>.....	72
8.63	net tahi reachable-time <lttime>.....	73
8.64	net tahi ping6 <ltip> <ltsize>.....	73
8.65	net tahi mping6 <ltmlip>.....	73
8.66	net tahi pmtu-route-add <ltipAdd>.....	73
8.67	net upnp configure.....	73
Chapter 9.	Configuration commands under branch SECURITY.....	74
9.1	security advanced_network attack_checks configure.....	74
9.2	security advanced_network igmp setup.....	74
9.3	security advanced_network igmp allowedsubnets add.....	75
9.4	security advanced_network igmp allowedsubnets edit <lthrow_id>.....	75
9.5	security advanced_network igmp allowedsubnets delete <lthrow_id>.....	75
9.6	security advanced_network ips setup.....	75
9.7	security application_rules add.....	76
9.8	security application_rules edit <lthrow_id>.....	76
9.9	security application_rules delete <lthrow_id>.....	77
9.10	security firewall custom_service add.....	77
9.11	security firewall custom_service edit <lthrow_id>.....	77
9.12	security firewall custom_service delete <lthrow_id>.....	77
9.13	security firewall ipv4 configure.....	78
9.14	security firewall ipv4 default_outbound_policy <ltdefault_outbound_policy>.....	79
9.15	security firewall ipv4 edit <lthrow_id>.....	79
9.16	security firewall ipv4 enable <lthrow_id>.....	80
9.17	security firewall ipv4 disable <lthrow_id>.....	80
9.18	security firewall ipv4 delete <lthrow_id>.....	80
9.19	security firewall ipv4 move <lthrow_id>.....	80
9.20	security firewall algs.....	81
9.21	security firewall ipv6 configure.....	81
9.22	security firewall ipv6 edit <lthrow_id>.....	82
9.23	security firewall ipv6 enable <lthrow_id>.....	83
9.24	security firewall ipv6 disable <lthrow_id>.....	83
9.25	security firewall ipv6 delete <lthrow_id>.....	83
9.26	security firewall ipv6 move <lthrow_id>.....	83
9.27	security firewall ipv6 default_outbound_policy <ltdefault_outbound_policy>.....	83
9.28	security ids configure.....	84
9.29	security session_settings configure.....	84

9.30	security schedules add	84
9.31	security schedules edit <ltrow_id>	85
9.32	security schedules delete <ltrow_id>	86
9.33	security mac_filter configure	86
9.34	security mac_filter source add	86
9.35	security mac_filter source edit <ltrow_id>	86
9.36	security mac_filter source delete <ltrow_id>	87
9.37	security ip_or_mac_binding add	87
9.38	security ip_or_mac_binding edit <ltrow_id>	87
9.39	security ip_or_mac_binding delete <ltrow_id>	87
9.40	security firewall vpn_passthrough configure	88
9.41	security website_filter content_filtering configure	88
9.42	security website_filter approved_urls add	88
9.43	security website_filter approved_urls edit <ltrow_id>	88
9.44	security website_filter approved_urls delete <ltrow_id>	89
9.45	security website_filter blocked_keywords add	89
9.46	security website_filter blocked_keywords edit <ltrow_id>	89
9.47	security website_filter blocked_keywords delete <ltrow_id>	89
9.48	security website_filter blocked_keywords enable <ltrow_id>	89
9.49	security website_filter blocked_keywords disable <ltrow_id>	90
Chapter 10.	Configuration commands under branch SYSTEM	91
10.1	system logging ipv4 configure	91
10.2	system logging facility configure <ltfacility>	92
10.3	system logging remote configure	92
10.4	system logging ipv6 configure	94
10.5	system remote_management https configure	94
10.6	system remote_management telnet configure	95
10.7	system snmp trap configure <ltagent_ip>	95
10.8	system snmp trap delete <ltagent_ip>	95
10.9	system snmp users configure <ltuser>	95
10.10	system snmp sys configure	96
10.11	system snmp access add	96
10.12	system snmp access edit <ltrowid>	96
10.13	system snmp access delete <ltrowid>	97
10.14	system switch_settings power_saving configure	97
10.15	system switch_settings jumbo_frame configure	97
10.16	system time configure	97
10.17	system traffic_meter configure	98
10.18	system usb usb1 configure	99
10.19	system usb usb2 configure	99
10.20	system usb shareport_vlan configure <ltrow_id>	99
10.21	system groups configure	99

10.22	system group add	100
10.23	system group edit <ltrow_id>.....	100
10.24	system group delete <ltrow_id>.....	100
10.25	system users add.....	100
10.26	system users edit <ltrow_id>	101
10.27	system users delete <ltrow_id>	101
10.28	system users password <ltuser>	101
10.29	system users idle_timeout <lttimeout>.....	101
10.30	system group groupaccesscontrol configure <ltgroup_id>.....	102
10.31	system group access_control_browser add	102
10.32	system group access_control_browser delete <ltrow_id>.....	102
10.33	system group access_control_ip add	102
10.34	system group access_control_ip delete <ltrow_id>	103
Chapter 11.	Configuration commands under branch DOT11	104
11.1	dot11 profile add <ltprofile_name>	104
11.2	dot11 profile edit <ltprofile_name>	104
11.3	dot11 radius configure.....	105
11.4	dot11 profile delete <ltprofile_name>	105
11.5	dot11 accesspoint configure <ltap_name>	105
11.6	dot11 accesspoint delete <ltap_name>	106
11.7	dot11 accesspoint disable <ltap_name>	106
11.8	dot11 accesspoint enable <ltap_name>	106
11.9	dot11 radio configure	106
11.10	dot11 radio advanced configure	107
11.11	dot11 accesspoint wps configure	107
11.12	dot11 accesspoint ACL configure <ltap_name>	107
11.13	dot11 accesspoint acl delete_mac_address <ltrowid>	108
Chapter 12.	Configuration commands under branch VPN.....	109
12.1	vpn l2tp server configure	109
12.2	vpn pptp client configure	109
12.3	vpn pptp client_action <ltaction>	110
12.4	vpn pptp server configure	110
12.5	vpn sslvpn portal-layouts add	111
12.6	vpn sslvpn portal-layouts edit <ltrow_id>.....	111
12.7	vpn sslvpn portal-layouts delete <ltrow_id>.....	112
12.8	vpn sslvpn portal-layouts set-default <ltrow_id>	112
12.9	vpn sslvpn portforwarding appconfig add.....	112
12.10	vpn sslvpn portforwarding appconfig delete <ltrow_id>	112
12.11	vpn sslvpn portforwarding hostconfig add	112
12.12	vpn sslvpn portforwarding hostconfig delete <ltrow_id>	113
12.13	vpn sslvpn resource add	113
12.14	vpn sslvpn resource configure add <ltresource_name>	113

12.15	vpn sslvpn resource configure delete <ltrow_id>	113
12.16	vpn sslvpn resource delete <ltrow_id>	114
12.17	vpn sslvpn policy add	114
12.18	vpn sslvpn policy edit <ltrow_id>	114
12.19	vpn sslvpn policy delete <ltrow_id>	115
12.20	vpn sslvpn client	115
12.21	vpn sslvpn route add	116
12.22	vpn sslvpn route delete <ltrow_id>	116
12.23	vpn sslvpn users domains add	116
12.24	vpn sslvpn users domains edit <ltdomain_Name>	117
12.25	vpn sslvpn users domains delete <ltdomainname>	118
12.26	vpn sslvpn users groups add	118
12.27	vpn sslvpn users groups edit <ltrow_id>	118
12.28	vpn sslvpn users groups delete <ltrow_id>	118
12.29	vpn sslvpn users users add	118
12.30	vpn sslvpn users users edit <ltrow_id>	119
12.31	vpn sslvpn users users login_policies <ltrow_id>	119
12.32	vpn sslvpn users users browser_policies <ltrow_id>	120
12.33	vpn sslvpn users users ip_policies configure <ltrow_id>	120
12.34	vpn sslvpn users users ip_policies delete <ltrow_id>	120
12.35	vpn sslvpn users users delete <ltrow_id>	121
12.36	vpn ipsec policy configure <ltname>	121
12.37	vpn ipsec policy enable <ltname>	125
12.38	vpn ipsec policy disable <ltname>	126
12.39	vpn ipsec policy delete <ltname>	126
12.40	vpn ipsec policy connect <ltname>	126
12.41	vpn ipsec policy drop <ltname>	126
Chapter 13.	Configuration commands under branch RADIUS	127
13.1	radius configure <ltradius_server>	127
13.2	radius delete <ltradius_server>	127

Chapter 1. Introduction

This document describes the command line interface (CLI) for managing D-Link's DSR-1000N/1000/500N/500/250N/250/150/150N series of routers.

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 DSR Unified Services Router cannot be managed by the CLI: Firmware Upgrade
- Configuration Backup / Restore
- Certificate Generate / Upload
- Power Savings mode configuration
- System Dashboard / Resource Utilization

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

1.1 Accessing the CLI

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

```
*****
```

```
Welcome to the DSR Command Line Interface
```

```
*****
```

```
D-Link DSR>
```

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

 *RIP, WAN2, DMZ, Captive Portal related commands are not available on DSR-250N/250/150/150N.*

 *Wireless related commands are available on DSR-1000N, DSR-500N, DSR-150N and DSR-250N only.*

Chapter 2. Basic commands available on the CLI

2.1 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.

2.2 AUTO-COMPLETION

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

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

2.3 MOVEMENT KEYS

- [CTRL-A] - 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.

2.4 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.

2.5 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 3. Command Hierarchy in CLI

3.1 CLI commands can be divided into 4 categories:

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

3.2 The router configuration is divided into 5 branches:

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

Chapter 4. Global commands used in CLI

- `.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 5. Show commands used in CLI

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

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:

SI No	Command Name	Purpose
1	<code>show net ipv6_tunnel status</code>	Display ipv6 tunnels status
2	<code>show net bandwidth</code>	.
3	<code>show net bandwidth profile</code>	.
4	<code>show net bandwidth profile setup</code>	Show list of Available Bandwidth Profile(s).
5	<code>show net bandwidth traffic_selector</code>	.
6	<code>show net bandwidth traffic_selector setup</code>	Show list of Available Traffic Selector(s).
7	<code>show net ddns</code>	.
8	<code>show net ddns setup</code>	Show Dynamic DNS Configuration.
9	<code>show net lan dhcp</code>	.
10	<code>show net lan dhcp reserved_ip</code>	.
11	<code>show net lan dhcp reserved_ip setup</code>	Show list of DHCP Reserved Addresses.
12	<code>show net lan dhcp leased_clients</code>	.
13	<code>show net lan dhcp leased_clients list</code>	Show list of Available DHCP Leased Clients.
14	<code>show net wan dhcpc</code>	Display dhcp client Configuration.
15	<code>show net dmz</code>	.
16	<code>show net dmz setup</code>	Show DMZ Configuration.
17	<code>show net dmz dhcp</code>	.
18	<code>show net dmz dhcp reserved_ip</code>	.
19	<code>show net dmz dhcp reserved_ip setup</code>	Show list of DMZ DHCP Reserved Addresses.
20	<code>show net dmz dhcp leased_clients</code>	.
21	<code>show net dmz dhcp leased_clients list</code>	Show list of Available DMZ DHCP Leased Clients.
22	<code>show net ethernet</code>	Show Ethernet interfaces
23	<code>show net lan</code>	.
24	<code>show net lan ipv4</code>	.
25	<code>show net lan ipv4 setup</code>	Show LAN Configuration.
26	<code>show net lan ipv6</code>	.
27	<code>show net lan ipv6 setup</code>	Show LAN Configuration.
28	<code>show net statistics <interface></code>	Show Interface Statistics
29	<code>show net intel_Amt</code>	show IntelAmt server details
30	<code>show net intel_Amt server</code>	show IntelAmt Server Configurations
31	<code>show net intel_Amt Reflector</code>	show IntelAmt Reflector Configuration
32	<code>show net intel_Amt server setup</code>	Display net Intel_Amt server setup.
33	<code>show net intel_Amt Reflector setup</code>	Display net Intel_Amt Reflector setup.
34	<code>show net lp_Alias</code>	show lp Alias server details
35	<code>show net lp_Alias server</code>	show lp Alias configuration details
36	<code>show net lp_Alias server setup</code>	Display net Intel_Amt server setup.
37	<code>show net mode</code>	.
38	<code>show net mode setup</code>	Display IP MODE configuration
39	<code>show net ipv6_tunnel</code>	.
40	<code>show net ipv6_tunnel setup</code>	Display ipv6 tunnels configuration
41	<code>show net routing mode</code>	.
42	<code>show net routing mode setup</code>	Routing Mode between WAN and LAN
43	<code>show net wan wan1</code>	.

44	show net wan wan1 ipv4	.
45	show net wan wan1 ipv4 status	Display ipv4 w an1 Information.
46	show net wan wan1 ipv4 setup	Display Wan1 Setup Information.
47	show net wan wan2	.
48	show net wan wan2 ipv4	.
49	show net wan wan2 ipv4 status	Display ipv4 w an2 Information.
50	show net wan wan2 ipv4 setup	Display w an2 Setup Information.
51	show net wan wan3	Display the w an3 configuration
52	show net wan wan3 threeG	Show wan3 configuration
53	show net wan wan3 threeG setup	Display w an3 Information.
54	show net wan wan3 threeG status	Display w an3 status.
55	show net wan	.
56	show net wan mode	Display w an mode Information.
57	show net wan port_setup	Display w an port Information.
58	show net wan configurable_port	Display configurable port Information.
59	show net wan wan1 ipv6	.
60	show net wan wan1 ipv6 status	Display ipv6 w an1 Information.
61	show net wan wan1 ipv6 setup	Display Wan1 Setup Information.
62	show net wan wan2 ipv6	.
63	show net wan wan2 ipv6 status	Display ipv6 w an2 Information.
64	show net wan wan2 ipv6 setup	Display Wan2 Setup Information.
65	show net routing ospfv2	show OSPFv2 Configuration
66	show net routing ospfv3	show OSPFv3 Configuration
67	show net routing ospfv2 setup	Display OSPFv2 Configuration
68	show net routing ospfv3 setup	Display OSPFv3 Configuration
69	show net port	.
70	show net port management	.
71	show net port management setup	Display port management configuration
72	show net wan pppoe	Display pppoe client Configuration.
73	show net routing protocol_binding	show protocol_binding rules
74	show net routing protocol_binding setup	Display protocol Binding Rules
75	show net radvd	.
76	show net radvd setup	Display RADVD configuration
77	show net routing dynamic	Show dynamic routing setup
78	show net routing dynamic setup	Show dynamic routing Setup.
79	show net routing	Displays routing setup
80	show net routing static	.
81	show net routing static ipv4	.
82	show net routing static ipv4 setup	Show all the configured IPV4 routes.
83	show net routing static ipv6	.
84	show net routing static ipv6 setup	Show all the configured IPV6 routes.
85	show net upnp	Display UPnP Information
86	show net upnp portmap	Display UPnP portmap Information.
87	show net upnp setup	Display UPnP portmap Information.

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:

SI No	Command Name	Purpose
1	show security advanced_network	show advanced firew all 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 advanced_network ips	Display ips configuration
5	show security application_rules	.
6	show security application_rules setup	Display application rules configuration

7	show security application_rules status	Display application rules status
8	show security firewall custom_service	.
9	show security firewall custom_service setup	Display Custom Service configuration
10	show security firewall	Display Firew all Rules
11	show security firewall ipv4	Display Firew all Rules
12	show security firewall ipv4 setup	Display Firew all Rules
13	show security firewall algs	Display ALGs protocols status
14	show security firewall ipv6	Display IPV6 Firew all Rules
15	show security firewall ipv6 setup	Display Firew all Rules
16	show security ids	.
17	show security ids setup	Display IDS configuration
18	show security session_settings	Display Session Settings configuration
19	show security schedules	.
20	show security schedules setup	Display Schedules configuration
21	show security mac_filter	.
22	show security mac_filter setup	Display Source Mac Filter configuration
23	show security ip_or_mac_binding	.
24	show security ip_or_mac_binding setup	Display IP/MAC Binding configuration
25	show security firewall vpn_passthrough	.
26	show security firewall vpn_passthrough setup	Display VPN passthrough Configuration
27	show security website_filter	.
28	show security website_filter content_filtering	Display content filtering configuration
29	show security website_filter approved_urls	Display trusted domains configuration
30	show security website_filter blocked_keywords	Display blocked keyw ords configuration

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 systemlogging	.
2	show systemlogging remote	.
3	show systemlogging remote setup	Display remote logging configuration
4	show systemlogging facility	.
5	show systemlogging facility setup <lfacility>	Display logging facility configuration
6	show systemlogging ipv4	.
7	show systemlogging ipv4 setup	Display logging configuration
8	show systemlogging ipv6	.
9	show systemlogging ipv6 setup	Display ipv6 logs configuration
10	show systemlog	Display captured log messages of the router activities
11	show systemlog all	Displays the all captured log messages of the router activities from Event Log. The logs displayed on this event viewer can be defined in the Log Configuration commands
12	show systemlog page	Displays Page Wise,captured log messages of the router activities from Event Log. The logs displayed on this event viewer can be defined in the Log Configuration commands
13	show systemremote_management	.
14	show systemremote_management setup	Display remote management over https configuration
15	show systemsnmp <ltagentIP>	Display SNMP configuration
16	show systemswitch_setting	.
17	show systemswitch_setting power_mode	Display pow er mode configuration
18	show systemswitch_setting jumbo_frame	Display jumbo frame configuration
19	show systemstatus	Display systemstatus
20	show systemtime	.
21	show systemtime setup	Display Timezone and NTP configuration
22	show systemtraffic_meter	.

23	show systemtraffic_meter setup	Display traffic meter configuration
24	show systemusb	Display USB Configuration
25	show systemusers	System group display mode
26	show systemgroup	System user display mode
27	show systemgroup specific <ltrow_id>	Display information for given group
28	show systemgroup all	Display all groups on system
29	show systemusers all	Display all users on system
30	show systemusers specific <ltrow_id>	Display information for given user
31	show systemgroup groupaccesscontrol <ltgroup_id>	Displays Group Access Control configuration for the selected group
32	show systemgroup access_control_browser	Displays Access Control browsers list
33	show systemgroup access_control_ip	Displays Access Control ips list
34	show systemfirmwareVersion	Get's the firmw are Version.

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

SI No	Command Name	Purpose
1	show dot11	Display 802.11 configuration
2	show dot11 accesspoint <ltap_name>	Display Access Point configuration. This command displays the list of configured Access Points for the device
3	show dot11 profile <ltprofile_name> <ltdisplay_qos>	Display Profile configuration
4	show dot11 statistics	Display access point and radio statistics
5	show dot11 acl <ltap_name>	Display access control list information for the specified access point.
6	show dot11 accesspoint status <ltap_name>	Display wireless stats.
7	show dot11 radius	Display radius Information.
8	show dot11 wps	Display WPS Information.
9	show dot11 wireless_statistics	Display wireless_statistics Information.
10	show dot11 radio	Display Radio configuration Available Radios This table shows the list of available radios that an AP may

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:

SI 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

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

SI No	Command Name	Purpose
1	show radius <ltserver>	Display radius configuration.

Chapter 6. Utility commands used in CLI

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

SI No	Command Name	Purpose
1	util ping	Ping or Trace an IP Address.
2	util restore_factory_defaults	Revert to factory default settings.
3	util reboot	Reboot the system

6.1 util system_check ping <ltip_address>

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

6.2 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

6.3 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

6.4 util system_check capturePackets start <ltinterface>

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

6.5 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

6.6 util cat <IfileName>

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

6.7 util md5sum <IfileName>

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

6.8 util copy <IfileName1> <IfileName2>

S.No	Command Name	Description	Type and Description
1	<IfileName1> <IfileName2>	Copy the Files.	String String

6.9 util usb_test <ItipAddr> <IfileName>

S.No	Command Name	Description	Type and Description
1	<ItipAddr> <IfileName>	To test the USB.	String String

Chapter 7. Configure commands used in CLI

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

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

SI No	Command Name	Description
1	<code>net ipv6_tunnel</code>	ipv6 tunnel configuration setup.
2	<code>net ipv6_tunnel six_to_four</code>	six to four tunnel configuration setup.
3	<code>net ipv6_tunnel six_to_four configure</code>	six To Four Tunnel configuration mode.
4	<code>net bandwidth</code>	.
5	<code>net bandwidth profile</code>	It gives options to add/edit/delete a bandwidth profile.
6	<code>net bandwidth profile enable <ltenable></code>	It allow s to enable/disable bandwidth profiles.
7	<code>net bandwidth profile add</code>	It allow s to add a bandwidth profile.
8	<code>net bandwidth profile edit <ltrow_id></code>	It allow s to edit a bandwidth profile.
9	<code>net bandwidth profile delete <ltrow_id></code>	It allow s to delete a bandwidth profile.
10	<code>net bandwidth traffic_selector</code>	It gives options to add/edit/delete a traffic selector for a bandwidth profile.
11	<code>net bandwidth traffic_selector add</code>	It allow s to add a traffic selector for a bandwidth profile.
12	<code>net bandwidth traffic_selector edit <ltrow_id></code>	It allow s to edit a traffic selector for a bandwidth profile.
13	<code>net bandwidth traffic_selector delete <ltrow_id></code>	It allow s to delete a traffic selector for a bandwidth profile.
14	<code>net ddns</code>	DDNS setup.
15	<code>net ddns wan1</code>	DDNS setup.
16	<code>net ddns wan2</code>	DDNS setup.
17	<code>net ddns wan1 configure</code>	DDNS configuration mode.
18	<code>net ddns wan2 configure</code>	DDNS configuration mode.
19	<code>net lan dhcp</code>	DHCP setup.
20	<code>net lan dhcp reserved_ip</code>	DHCP Reserved IPs setup.
21	<code>net lan dhcp reserved_ip configure <ltmac_address></code>	DHCP Reserved IPs add/edit mode.
22	<code>net lan dhcp reserved_ip delete <ltmac_address></code>	Delete a specific reserved ip entry.
23	<code>net wan dhcpc</code>	DHCP client configuration mode
24	<code>net wan dhcpc configure</code>	DHCP client configuration mode
25	<code>net dmz</code>	dmz configuration mode
26	<code>net dmz configure</code>	dmz configuration mode
27	<code>net dmz dhcp</code>	DHCP setup.
28	<code>net dmz dhcp reserved_ip</code>	DHCP Reserved IPs setup.
29	<code>net dmz dhcp reserved_ip configure <ltmac_address></code>	DHCP Reserved IPs add/edit mode.
30	<code>net dmz dhcp reserved_ip delete <ltmac_address></code>	Delete a specific reserved ip entry.
31	<code>net ethernet</code>	Ethernet configuration.
32	<code>net ethernet configure <ltinterface_name></code>	Ethernet configuration mode.
33	<code>net lan</code>	LAN setup.

34	net lan ipv4	.
35	net lan ipv4 configure	IPv4 LAN configuration mode.
36	net lan ipv6	.
37	net lan ipv6 configure	IPv6 LAN configuration mode.
38	net lan ipv6 pool	.
39	net lan ipv6 pool configure <ltipv6PoolStartAddr>	IPv6 LAN configuration add/edit mode.
40	net lan ipv6 pool delete <ltipv6PoolStartAddr>	IPv6 LAN configuration delete.
41	net intel_Amt	net policy mode.
42	net intel_Amt server	net policy mode.
43	net intel_Amt server configure	Intel Amt server configuration mode
44	net intel_Amt_Reflecto	net policy mode.
45	net intel_Amt_Reflecto configure	Intel Amt Reflector configuration mode
46	net ip_Aliasing	net policy mode.
47	net ip_Aliasing server	net policy mode.
48	net ip_Aliasing server add	Ip Aliasing server configuration
49	net ip_Aliasing server edit <ltrow_id>	Editing Ip Aliasing server configuration.
50	net ip_Aliasing server delete <ltrow_id>	Delete Ip Aliasing configuratio
51	net mode	IP Mode Setup
52	net mode configure	IP Mode configuration mode.
53	net ipv6_tunnel isatap	isatap tunnel configuration setup.
54	net ipv6_tunnel isatap add	isatap tunnel configuration mode.
55	net ipv6_tunnel isatap edit <ltrow_id>	isatap Tunnel configuration mode.
56	net ipv6_tunnel isatap delete <ltrow_id>	isatap tunnel configuration mode.
57	net routing mode	Routing Mode between WAN and LAN setup.
58	net routing mode configure	Routing Mode between WAN and LAN configuration mode.
59	net w an wan1	w an configuration mode
60	net w an wan1 ipv4	ipv4 wan configuration mode
61	net w an wan1 ipv4 configure	ipv4 wan wan1 configuration mode
62	net w an wan2	w an configuration mode
63	net w an wan2 ipv4	ipv4 wan configuration mode
64	net w an wan2 ipv4 configure	ipv4 wan wan2 configuration mode
65	net w an wan3	w an3 configuration mode
66	net w an wan3 threeG	w an3 configuration mode
67	net w an wan3 threeG configure	threeG wan wan3 configuration mode
68	net w an	w an mode configuration mode
69	net w an mode	w an mode configuration mode
70	net w an mode configure	w an mode configuration mode
71	net w an port_setup	w an port setup.
72	net w an port_setup configure	w an port configuration mode.
73	net w an configurable_port	configurable port setup.
74	net w an configurable_port configure	configurable port setup.
75	net w an wan1 ipv6	ipv6 wan configuration mode
76	net w an wan1 ipv6 configure	ipv6 wan1 configuration mode
77	net w an wan2 ipv6	ipv6 wan2 configuration mode
78	net w an wan2 ipv6 configure	ipv6 wan2 configuration mode
79	net routing ospfv2	OSPF Configuration for IPV 4
80	net routing ospfv3	OSPF Configuration for IPV 6
81	net routing ospfv2 configure <ltinterface>	ospfv2 configuration mode.
82	net routing ospfv3 configure <ltinterface>	ospfv3 configuration mode.
83	net port	.
84	net port management	port management configuration setup.
85	net port management configure	port management configuration mode.

	<ltportName>	
86	net wan pppoe	PPPOE client configuration mode
87	net wan pppoe configure	PPPOE client configuration mode
88	net routing protocol_binding	protocol_binding rules
89	net routing protocol_binding add	protocol_binding rules configuration mode.
90	net routing protocol_binding edit <ltrow_id>	protocol_binding rules configuration mode.
91	net routing protocol_binding enable <ltrow_id>	protocol_binding rules configuration mode.
92	net routing protocol_binding disable <ltrow_id>	protocol_binding rules configuration mode.
93	net routing protocol_binding delete <ltrow_id>	protocol_binding rules configuration mode.
94	net radvd	RADVD configuration setup.
95	net radvd pool	RADVD configuration setup.
96	net radvd configure	radvd configuration mode.
97	net radvd pool add	radvd Pool configuration mode.
98	net radvd pool edit <ltrow_id>	radvd Pool configuration mode.
99	net radvd pool delete <ltrow_id>	radvd pool configuration mode.
100	net routing dynamic	Configure the routes dynamically.
101	net routing dynamic configure	configure the routes dynamically.
102	net routing	configure routing mode, static and dynamic route(s).
103	net routing static	Configure the routes.
104	net routing static ipv4	Configure the routes.
105	net routing static ipv6	Configure the IPV6 routes.
106	net routing static ipv4 configure <ltname>	Add new static routes.
107	net routing static ipv6 configure <ltname>	Add new IPV6 static routes.
108	net routing static ipv4 delete <ltname>	Delete a specific route.
109	net routing static ipv6 delete <ltname>	Delete a specific IPV6 route.
110	net routing static ipv4 deleteAll	Delete all the configured routes.
111	net routing static ipv6 deleteAll	Delete all the configured IPV6 routes.
112	net tahi	settings for tahi test suite.
113	net tahi add-default-route <ltip_address>	add ipv6 default route on lan interface.
114	net tahi delete-default-route	delete ipv6 default route on lan interface.
115	net tahi add-route <ltip_address> <ltgw>	add ipv6 route on lan interface.
116	net tahi del-route <ltip_address> <ltgw>	add ipv6 route on lan interface.
117	net tahi stop-RA	stop sending RA.
118	net tahi start-RA-AdvRetransTimer(1000)	start sending RA with AdvRetransTimer as 1000.
119	net tahi start-RA-AdvRetransTimer(5000)	start sending RA with AdvRetransTimer as 5000.
120	net tahi startRA-Reachable(30000)Retrans(1000)	start sending RA with AdvReachableTime as 30000 and AdvRetransTimer as 1000.
121	net tahi start-RA-AdvReachableTime(10000)	start sending RA with AdvReachableTime as 10000.
122	net tahi start-RA-AdvReachableTime(30000)	start sending RA with AdvReachableTime as 30000.
123	net tahi start-RA(Default)	start sending RA with default parameters.
124	net tahi start-RA-MinValues	start sending RA with minimum values of parameters.
125	net tahi start-RA-MaxValues	start sending RA with maximum values of parameters.
126	net tahi start-RA-MaxRtrAdvInterval(10)	start sending RA with MaxRtrAdvInterval value of 10.
127	net tahi start-RA-MaxRtrAdvInterval(40)	start sending RA with MaxRtrAdvInterval value of 40.
128	net tahi start-RA-MinRtrAdvInterval(198)	start sending RA with MinRtrAdvInterval value of 198.
129	net tahi start-RA-prefix(8000::)	start sending RA with prefix 8000::/64.
130	net tahi start-RA-prefix(fec0::)	start sending RA with prefix fec0::/64.
131	net tahi start-RA-AdvCurHopLimit(0)	start sending RA with AdvCurHopLimit value as 0.
132	net tahi start-RA-AdvCurHopLimit(15)	start sending RA with AdvCurHopLimit value as 15.
133	net tahi start-RA-WAN	start sending RA on the WAN interface.
134	net tahi ipv6-down	disable the ipv6 stack on the router.

135	net tahi ipv6-up	enable the ipv6 stack on the router.
136	net tahi ipv6-global-up	enable the ipv6 stack on the router and adds global ip.
137	net tahi ipv6-Alias-Add(LAN) <ltip6_address>	Add ipv6 address to LAN interface.
138	net tahi ipv6-Alias-Del(LAN) <ltip6_address>	Delete an ipv6 address from LAN interface.
139	net tahi ipv6-Alias-Add(WAN) <ltip6_address>	Add ipv6 address to WAN interface.
140	net tahi ipv6-Alias-Del(WAN) <ltip6_address>	Delete an ipv6 address from WAN interface.
141	net tahi neigh-cache-del	deletes the ipv6 neighbor cache.
142	net tahi reachable-time <ltime>	set the reachable time of neighbour cache entries
143	net tahi mcast-start	start ipv6 multicast
144	net tahi mcast-stop	stop ipv6 multicast
145	net tahi ping6 <ltip> <ltsize>	ping6 on LAN interface with count one
146	net tahi mping6 <ltmp>	multicast ping6
147	net tahi pmtu-route-add <ltipAdd>	add ipv6 route on lan interface.
148	net tahi disable-ipv6-firewall	disable ipv6 firewall.
149	net tahi show -LAN-ip	show ipv6 addresses of LAN interface.
150	net upnp	Upnp configuration mode
151	net upnp configure	Upnp configuration mode

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

SI No	Command Name	Description
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 allow edsubnets	Configure network address of multicast source.
6	security advanced_network igmp setup	igmp configuration mode.
7	security advanced_network igmp allow edsubnets add	Add network address and mask length of multicast source
8	security advanced_network igmp allow edsubnets edit <lrow_id>	Edit network address and mask length of multicast source
9	security advanced_network igmp allow edsubnets delete <lrow_id>	delete network address and mask length of multicast source
10	security advanced_network ips	Security ips setup.
11	security advanced_network ips setup	ips configuration mode.
12	security application_rules	Application Rules Configuration setup.
13	security application_rules add	application rules rules configuration mode.
14	security application_rules edit <lrow_id>	application rules rules configuration mode.
15	security application_rules delete <lrow_id>	application rules rules configuration mode.
16	security firewall custom_service	Custom Services Configuration setup.
17	security firewall custom_service add	customservices configuration mode.
18	security firewall custom_service edit <lrow_id>	customservices configuration mode.
19	security firewall custom_service delete <lrow_id>	customservices configuration mode.
20	security firewall	Firewall rules setup.
21	security firewall ipv4	Firewall IPv4 rules setup.
22	security firewall ipv4 configure	Firewall IPv4 rules configuration mode.
23	security firewall ipv4 default_outbound_policy <ldefault_outbound_policy>	Firewall Settings, Default Outbound Policy configuration mode.
24	security firewall ipv4 edit <lrow_id>	Firewall IPv4 rules configuration mode.

25	security firewall ipv4 enable <ltrow_id>	Firewall IPv4 rules configuration mode.
26	security firewall ipv4 disable <ltrow_id>	Firewall IPv4 Rules configuration mode.
27	security firewall ipv4 delete <ltrow_id>	Firewall IPv4 Rules configuration mode.
28	security firewall ipv4 move <ltrow_id>	Firewall IPv4 Rule reordering mode.
29	security firewall algs	Firewall ALGs configuration mode.
30	security firewall ipv6	Firewall IPv6 rules setup.
31	security firewall ipv6 configure	Firewall IPv6 rules configuration mode.
32	security firewall ipv6 edit <ltrow_id>	Firewall IPv6 rules configuration mode.
33	security firewall ipv6 enable <ltrow_id>	Firewall IPv6 rules configuration mode.
34	security firewall ipv6 disable <ltrow_id>	Firewall IPv6 Rules configuration mode.
35	security firewall ipv6 delete <ltrow_id>	Firewall IPv6 Rules configuration mode.
36	security firewall ipv6 move <ltrow_id>	Firewall IPv6 Rule reordering mode.
37	security firewall ipv6 default_outbound_policy <ltdefault_outbound_policy>	Firewall Settings, IPv6 Default Outbound Policy configuration mode.
38	security ids	IDS Configuration setup.
39	security ids configure	IDS configuration mode.
40	security session_settings	Session Settings Configuration setup.
41	security session_settings configure	Session Settings configuration mode.
42	security schedules	Schedules Configuration setup.
43	security schedules add	Schedules configuration mode.
44	security schedules edit <ltrow_id>	Schedules configuration mode.
45	security schedules delete <ltrow_id>	Schedules configuration mode.
46	security mac_filter	source mac filter configuration mode.
47	security ip_or_mac_binding	ip mac binding configuration mode.
48	security mac_filter configure	source mac filter configuration mode.
49	security mac_filter source	.
50	security mac_filter source add	Source Mac Filter configuration mode.
51	security mac_filter source edit <ltrow_id>	Source Mac Filter configuration mode.
52	security mac_filter source delete <ltrow_id>	Source Mac Filter configuration mode.
53	security ip_or_mac_binding add	ip/mac binding configuration mode.
54	security ip_or_mac_binding edit <ltrow_id>	ip/mac binding configuration mode.
55	security ip_or_mac_binding delete <ltrow_id>	ip/mac binding configuration mode.
56	security firewall vpn_passthrough	VPN Passthrough setup.
57	security firewall vpn_passthrough configure	VPN Passthrough configuration mode.
58	security website_filter	website filtering configuration setup.
59	security website_filter content_filtering	content filtering configuration setup.
60	security website_filter approved_urls	trusted domains configuration setup.
61	security website_filter blocked_keywords	blocked keywords configuration setup.
62	security website_filter content_filtering configure	content filtering configuration mode.
63	security website_filter approved_urls add	trusted domains configuration mode.
64	security website_filter approved_urls edit <ltrow_id>	trusted domains configuration mode.
65	security website_filter approved_urls delete <ltrow_id>	trusted Domains configuration mode.
66	security website_filter blocked_keywords add	blocked Keyword configuration mode.
67	security website_filter blocked_keywords edit <ltrow_id>	blocked Keywords configuration mode.
68	security website_filter blocked_keywords delete <ltrow_id>	blocked Keywords configuration mode.
69	security website_filter blocked_keywords enable <ltrow_id>	blocked Keywords configuration mode.
70	security website_filter blocked_keywords disable <ltrow_id>	blocked Keywords configuration mode.

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

SI No	Command Name	Purpose
1	systemlogging facility configure <facility_type>	Facility logging configuration mode
2	systemlogging ipv4 configure	Firewall all ipv4 logs configuration mode
3	systemlogging ipv6 configure	Firewall all ipv6 logs configuration mode
4	systemlogging remote configure	Remote logging configuration mode
5	systemradius configure <radius_server>	Radius configuration mode
6	systemradius delete <radius_server>	Radius configuration delete mode
7	systemremote_management https configure	Remote management configuration mode
8	systemsntp sys configure	Ntp system configuration mode
9	systemsntp trap configure <agent_ip>	Ntp trap configuration mode
10	systemsntp trap delete <agent_ip>	Ntp trap configuration delete mode
11	systemtime configure	Ntp time configuration mode
12	systemtraffic_meter configure	Traffic meter configuration mode
13	systemusers idle_timeout <timeout>	Admin idle timeout configuration
14	systemusers password <user_string>	Users password configuration

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

I 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 <ltdomain_Name>	Users domain configuration mode
43	vpn sslvpn users domains delete <ltdomainname>	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

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

SI No	Command Name	Purpose
1	<code>dot11 access point configure</code>	802.11 access point configuration mode
2	<code>dot11 access point delete</code>	Delete an 802.11 access point.
3	<code>dot11 access point disable</code>	Disable an 802.11 access point.
4	<code>dot11 access point enable</code>	Enable an 802.11 access point.
5	<code>dot11 access point mac add</code>	Add a MAC Address to ACL List of an AP
6	<code>dot11 access point mac delete</code>	Delete a MAC Address froman ACL List of an AP.
7	<code>dot11 radio advanced configure</code>	802.11 advanced radio configuration mode.
8	<code>dot11 radio configure</code>	802.11 radio configuration mode.
9	<code>dot11 profile configure</code>	802.11 profile configuration mode.
10	<code>dot11 profile delete</code>	Delete an 802.11 profile.

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

SI No	Command Name	Description
1	<code>radius configure <radius_server></code>	RADIUS configuration mode.
2	<code>radius delete <radius_server></code>	Delete a RADIUS configuration mode.

Each of the above listed commands has in turn a set of sub-commands to fulfill the requirements. The command – subcommand list is given in following sections.

Chapter 8. Configuration commands under branch NET

8.1 net bandwidth profile enable

SI No	Command Name	Description	Type and Description
1	enable	Enable or disable bandwidth profiles	Boolean (Y/N) Enable/ Disable bandwidth profiles

8.2 net bandwidth profile add/edit

SI No	Command Name	Description	Type and Description
1	cancel	Roll back bandwidth Profile configuration changes.	
2	exit	Save bandwidth Profile configuration changes and exit current mode.	
3	maximum_rate	Maximum Bandwidth provided by user.	Maximum Bandwidth rate 100-100000 Kbps
4	minimum_rate	Minimum Bandwidth provided by user	Minimum Bandwidth provided by user. (0..100000)
5	name	Unique Profile Name.	STRING, profile name
6	priority	Priority.	Priority type (low/medium/high)
7	save	Save bandwidth profile configuration changes.	
8	type	Profile Type, either Priority or Rate	Profile type (Priority/Rate)
9	wan_interface	Wan interface provided by user.	WAN interface type

8.3 net bandwidth profile delete <row_id>

SI No	Command Name	Description	Type and Description
1	row_id	Row Id of the bandwidth profile to be deleted	Unsigned integer Row id number

8.4 net bandwidth traffic_selector add

S.No	Command Name	Description	Type and Description
1	save	Save Traffic Selector configuration changes.	
2	exit	Save Traffic Selector configuration changes and exit current mode.	
3	cancel	Roll back Traffic Selector configuration changes.	
4	profile_name	Profile Name.	String
5	service_name	Service Name.	String
6	match_type	IP /MAC Address	traffic selector match type
7	ip_address	IP Address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
8	mac_address	MAC Address	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
9	port_name	Port Name	traffic selectors Port types
10	vlan_id	Vlan ID	Unsigned integer

8.5 net bandwidth traffic_selector edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	It allow s to edit a traffic selector for a bandwidth profile.	Unsigned integer
2	save	Save Traffic Selector configuration changes.	
3	exit	Save Traffic Selector configuration changes and exit current mode.	
4	cancel	Roll back Traffic Selector configuration changes.	
5	profile_name	Profile Name.	String
6	service_name	Service Name.	String
7	match_type	IP /MAC Address	traffic selector match type
8	ip_address	IP Address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
9	mac_address	MAC Address	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF
10	port_name	Port Name	traffic selectors Port types
11	vlan_id	Vlan ID	Unsigned integer

8.6 net bandwidth traffic_selector delete <ltrow_id>

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

8.7 net ddns wan1 configure

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

8.8 net ddns wan2 configure

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

8.9 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 w here each part is in the range 0-255

8.10 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 w here each part is in the range 00-FF

8.11 net wan 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 w here each part is in the range 0-255
6	SecondaryDns	Set Secondary DNS server	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

8.12 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 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
6	dhcp_mode	Set DHCP mode.	dhcpv4 modes
7	starting_ip_address	DHCP Starting IP address.	IP address AAA.BBB.CCC.DDD w here each part is in the range

			0-255
8	ending_ip_address	DHCP ending IP address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
9	primary_dns_server	Primary DNS address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
10	secondary_dns_server	Secondary DNS server address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
11	wins_server	Set DHCP WINS server.	IP address AAA.BBB.CCC.DDD w here 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 w here 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 w here each part is in the range 0-255

8.13 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 w here 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 w here each part is in the range 0-255

8.14 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 w here each part is in the range 00-FF

8.15 net ethernet configure <ltinterface_name>

S.No	CommandName	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

8.16 net lan ipv4 configure

S.No	CommandName	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 w here each part is in the range 0-255
6	static subnet_mask	Set system LAN subnet mask.	IP address AAA.BBB.CCC.DDD w here 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 w here each part is in the range 0-255
10	dhcp end_address	Set dhcp servers end address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
11	dhcp default_gw	Set dhcp default gateway.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
12	dhcp primary_dns	Set primary dns server.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
13	dhcp secondary_dns	Set secondary dns server.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
14	dhcp w ins_server	Set Wins Server address.	IP address AAA.BBB.CCC.DDD w here 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 w here each part is in the range 0-255
18	dns	Configure DNS Settings.	

19	dns host_name	Configure DNS Settings.	
20	dns host_name mapping	Configure DNS Host NameMapping.	
21	dns host_name mapping 1	Configure DNS Host NameMapping for 1st row .	
22	dns host_name mapping 2	Configure DNS Host NameMapping for 2nd Row .	
23	dns host_name mapping 3	Configure DNS Host NameMapping for 3rd row .	
24	dns host_name mapping 4	Configure DNS Host NameMapping for 4th row .	
25	dns host_name mapping 5	Configure DNS Host NameMapping for 5th row .	
26	dns host_name mapping 6	Configure DNS Host NameMapping for 6th row .	
27	dns host_name mapping 7	Configure DNS Host NameMapping for 7th row .	
28	dns host_name mapping 8	Configure DNS Host NameMapping for 8th row .	
29	dns host_name mapping 1 host_name	Set Host Name.	String
30	dns host_name mapping 1 ipaddress	Set Host Name.	IP address AAA.BBB.CCC.DDD w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here each part is in the range 0-255
45	proxy	Configure the LAN Proxies	
46	proxy dns_enable	Enable/Disable dns proxy	Boolean choice

8.17 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

8.18 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 w here each part is in the range [0-9A-Fa-f:]
7	prefix_value	Prefix length	Unsigned integer

8.19 net lan ipv6 pool delete <ltipv6PoolStartAddr>

S.No	CommandName	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:]

8.20 net intel_Amt server configure

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

8.21 net intel_Amt_Reflector configure

S.No	CommandName	Description	Type and Description
1	save	Save InterIAmt 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_Reflecto... 16995	enable/disable Ports.	Boolean choice
11	enable Intel_Amt_Reflecto... 9971	enable/disable Ports.	Boolean choice
12	Intel_Amt_Reflecto... srcport	set port number for different ports	
13	Intel_Amt_Reflecto... 16992	Enter source port value for 16992	Port number
14	Intel_Amt_Reflecto... 16993	Enter source port value for 16993	Port number
15	Intel_Amt_Reflecto... 16994	Enter source port value for 16994	Port number
16	Intel_Amt_Reflecto... 16995	Enter source port value for 16995	Port number
17	Intel_Amt_Reflecto... 9971	Enter source port value for 9971	Port number

8.22 net ip_Aliasing server add

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

8.23 net ip_Aliasing server edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	Editing Ip Aliasing server configuration.	Unsigned integer
2	save	Save Ip Alias server configuration changes.	
3	cancel	Roll back Ip Alias server configuration changes.	
4	exit	Save Ip Alias server configuration changes and exit current mode.	
5	Interface	Select the Interface for the Ip Aliasing	WAN interface type
6	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD 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

8.24 net ip_Aliasing server delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	Delete Ip Aliasing configuratio	

			Unsigned integer
2	save	Save Ip Alias server configuration changes.	
3	cancel	Roll back Ip Alias server configuration changes.	
4	exit	Save Ip Alias server configuration changes and exit current mode.	
5	Interface	Select the Interface for the Ip Aliasing	WAN interface type
6	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD 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

8.25 net mode configure

S.No	CommandName	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

8.26 net ipv6_tunnel isatap add

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

8.27 net ipv6_tunnel isatap edit <ltrow_id>

S.No	CommandName	Description	Type and Description
1	<ltrow_id>	isatap Tunnel configuration mode.	Unsigned integer
2	save	Save isatap tunnel configuration changes.	
3	exit	Save isatap tunnel configuration changes and exit current mode.	
4	cancel	Roll back isatap tunnel configuration	

		changes.	
5	subnet_prefix	This is the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet.	String
6	end_point_type	This is the endpoint address for the tunnel that starts with this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 network), or a specific LAN IPv4 address	select the local end point address type
7	ipv4_address	The local end point address if not the LAN IPv4 address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

8.28 net ipv6_tunnel isatap delete <ltrow_id>

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

8.29 net routing mode configure

S.No	CommandName	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

8.30 net wan wan1 ipv4 configure

S.No	CommandName	Description	Type and Description
1	save	Save ipv4 wan configuration changes.	
2	cancel	Roll back ipv4 wan configuration changes.	
3	exit	Save ipv4 wan 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, Dual Access Pppoe	ISP Types.
5	dhcpc	If ISP Type selected is DHCPC, this field gives you options to configure DHCPC credentials	
6	dhcpc get_dns_from_osp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign a DNS address to the router using DHCP network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
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

			w here 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 w here 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 w here 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 w here each part is in the range 0-255
15	static gateway_address	IP address of the ISP's gateway. This is usually provided by the ISP or your network administrator.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
16	static primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
17	static secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here 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 w here 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

			w here each part is in the range 0-255
29	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here 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 w here each part is in the range 0-255
32	pppoe subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD w here 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 w here 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 w here 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 w here 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 w here 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 w here 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	Boolean choice

		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	
48	pptp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
49	pptp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here 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 w here 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 w here 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 w here 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 w here 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 w here 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

			w here each part is in the range 0-255
66	russ_pppt secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
67	russ_pppt mac_type	Select the Mac Address Source	Types of mac address source
68	russ_pppt mac_address	enter Valid MAC address	MAC address AA:BB:CC:DD:EE:FF w here 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 w here 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 w here 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 w here 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 w here 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 w here each part is in the range 0-255
83	l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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	Boolean choice

		protocol. Otherwise Enter No and give valid static dns addresses	
125	japanese_pppoe secondary_profile primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here 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 w here 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 w here each part is in the range 0-255
129	japanese_pppoe secondary_profile subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD w here 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 w here each part is in the range 00-FF
132	dual_pppoe	If ISP Type selected is Dual PPPoE, this field gives you options to configure Dual Access PPPoE credentials	
133	dual_pppoe username	Enter the username to authenticate	String
134	dual_pppoe password	Enter the password to authenticate	String
135	dual_pppoe service	Enter the service to authenticate	String
136	dual_pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
137	dual_pppoe connectivity_type	Enter the connectivity type	ISP Connectivity Types.
138	dual_pppoe idletime	Enter the idle time	idle timeout value type.
139	dual_pppoe get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static Dns address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
140	dual_pppoe primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
141	dual_pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
142	dual_pppoe get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically	Boolean choice

		assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	
143	dual_pppoe static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
144	dual_pppoe subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
145	dual_pppoe get_ip_from_phy	Enter Yes to get ip on physical interface from dhcp server in the internal isp network. Otherwise Enter No and give valid static IP address, subnet mask and gateway	Boolean choice
146	dual_pppoe static_ip_phy	Valid IP Address of physical interface	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
147	dual_pppoe subnet_mask_phy	Valid subnet mask of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
148	dual_pppoe gateway_phy	Valid gateway of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
149	dual_pppoe get_dns_from_isp_phy	Enter Yes to get dns dynamically from internal ISP if you have not been assigned any static Dns address. The internal ISP will automatically assign a DNS address to the router using Dhcp network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
150	dual_pppoe primary_dns_phy	Valid primary DNS Server IP Address of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
151	dual_pppoe secondary_dns_phy	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

8.31 net wan wan2 ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Save ipv4 wan configuration changes.	
2	cancel	Roll back ipv4 wan configuration changes.	
3	exit	Save ipv4 wan 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, Dual Access Pppoe	WAN2 ISP Types.
5	dhcpc	If ISP Type selected is DHCP, this field gives you options to configure DHCP 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	Boolean choice

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

		valid static IP address	
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	Boolean choice

		dns addresses	
82	l2tp primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
83	l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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

			w here 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 w here 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 w here 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 w here 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 w here each part is in the range 0-255
116	japanese_pppoe primary_profile subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD w here 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
132	dual_pppoe	If ISP Type selected is Dual PPPoE, this field gives you options to configure Dual Access PPPoE credentials	
133	dual_pppoe username	Enter the username to authenticate	String
134	dual_pppoe password	Enter the password to authenticate	String
135	dual_pppoe service	Enter the service to authenticate	String
136	dual_pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
137	dual_pppoe connectivity_type	Enter the connectivity type	ISP Connectivity Types.
138	dual_pppoe idletime	Enter the idle time	idle timeout value type.
139	dual_pppoe get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static Dns address. The ISP will automatically assign an DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
140	dual_pppoe primary_dns	Valid primary DNS Server IP Address	

			IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
141	dual_pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
142	dual_pppoe get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using PPPOE network protocol. Otherwise Enter No and give valid static IP address	Boolean choice
143	dual_pppoe static_ip	Valid IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
144	dual_pppoe subnet_mask	Valid subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
145	dual_pppoe get_ip_from_phy	Enter Yes to get ip on physical interface from dhcp server in the internal isp network. Otherwise Enter No and give valid static IP address, subnet mask and gateway	Boolean choice
146	dual_pppoe static_ip_phy	Valid IP Address of physical interface	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
147	dual_pppoe subnet_mask_phy	Valid subnet mask of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
148	dual_pppoe gateway_phy	Valid gateway of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
149	dual_pppoe get_dns_from_isp_phy	Enter Yes to get dns dynamically from internal ISP if you have not been assigned any static Dns address. The internal ISP will automatically assign an DNS address to the router using Dhcp network protocol. Otherwise Enter No and give valid static dns addresses	Boolean choice
150	dual_pppoe primary_dns_phy	Valid primary DNS Server IP Address of physical network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
151	dual_pppoe secondary_dns_phy	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

8.32 net wan wan3 threeG configure

S.No	CommandName	Description	Type and Description
1	save	Save wan3 threeG configuration changes.	
2	cancel	Roll back wan3 threeG configuration changes.	
3	exit	Save wan3 threeG configuration changes and current mode.	

4	Username	Enter the username required to log in to the ISP.	String
5	Passw ord	Enter the passw ord required to login to the ISP	String
6	Dial_number	Enter the number to dial to the ISP	String
7	AuthMethod	Select one of None, PAP or CHAP Authentication Protocols to connect to the ISP	THREEEG Authentication Types.
8	Apn	Enter the APN(Access Point Name) provided by the ISP	String
9	Reconnect_mode	Select Alw ays On: The connection is alw ays on OR On Demand :The connection w ill close after time specified in Idle_time field	ISP Connectivity Types.
10	Idle_time	The connection is automatically ended if it is idle for a specified number of minutes	idle timeout value type.
11	Get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP w ill automatically assign an DNS address to the router using THREEEG netw ork protocol. Otherw ise Enter No and give valid static dns addresses	Boolean choice
12	Primary_dns	Valid primary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
13	Secondary_dns	Valid secondary DNS Server IP Address	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

8.33 net wan mode configure

S.No	CommandName	Description	Type and Description
1	save	Save w an mode configuration changes.	
2	cancel	Roll back ipv4 w an configuration changes.	
3	exit	Save w an mode configuration changes and current mode.	
4	w an_mode_type	Select among the options: SINGLE_WAN, LOAD_BALANCING, AUTO_ROLLOVER	Types of WAN 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 bandw idth after which the router sw itches to secondary WAN	Unsigned integer
10	loadbalancing spillover max_bandw idth	Sets the maximum bandw idth tolerable by the Primary WAN.If the bandw idth goes below the load tolerance value of configured Max Bandw idth, the router sw itches to secondary WAN.	Unsigned integer
11	loadbalancing failover_method type	Select the Fail Over detection method	Types of Failover Detection

			methods
12	loadbalancing failover_method dns		
13	loadbalancing failover_method dns ipaddr_w an1		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
14	loadbalancing failover_method dns ipaddr_w an2		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
15	loadbalancing failover_method dns ipaddr_w an3		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
16	loadbalancing failover_method ping		
17	loadbalancing failover_method ping ipaddr_w an1		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
18	loadbalancing failover_method ping ipaddr_w an2		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
19	loadbalancing failover_method ping ipaddr_w an3		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
20	loadbalancing failover_method retry_interval		idle timeout value type.
21	loadbalancing failover_method retry_attempts		number in range of 2 to 999
22	rollover	Wan Mode in Auto Rollover	
23	rollover w an_port	Select the Auto rollover WAN port	WAN interface type
24	rollover w an_port_Sec	Select the Auto rollover WAN port	WAN interface type
25	rollover failover_method	Select the Fail Over detection method	
26	rollover failover_method type	Select the Fail Over detection method	Types of Failover Detection methods
27	rollover failover_method dns		
28	rollover failover_method dns ipaddr_w an1		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
29	rollover failover_method dns ipaddr_w an2		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
30	rollover failover_method dns ipaddr_w an3		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
31	rollover failover_method ping		
32	rollover failover_method ping ipaddr_w an1		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
33	rollover failover_method ping ipaddr_w an2		IP address AAA.BBB.CCC.DDD

			w here each part is in the range 0-255
34	rollover failover_method ping ipaddr_w an3		IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
35	rollover failover_method retry_interval		idle timeout value type.
36	rollover failover_method retry_attempts		number in range of 2 to 999
37	singleport		
38	singleport w an_port		WAN interface type

8.34 net wan port_setup configure

S.No	CommandName	Description	Type and Description
1	save	Save WAN port settings.	
2	exit	Save WAN port settings and exit current mode.	
3	cancel	Roll back WAN port settings changes.	
4	respond_ping	Disable or Enable ping on WAN side	Boolean choice
5	w an1	WAN1 port settings	
6	w an1 mtu_type	Enter MTU type	mtu type
7	w an1 mtu_size	Enter MTU size for WAN1	mtu size
8	w an1 port_speed	Enter the type of port speed for WAN1	Port Speed types
9	w an2	WAN2 port settings	
10	w an2 mtu_type	Enter MTU type	mtu type
11	w an2 mtu_size	Enter MTU size for WAN2	mtu size
12	w an2 port_speed	Enter the type of port speed for WAN2	Port Speed types

8.35 net wan configurable_port configure

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

8.36 net wan wan1 ipv6 configure

S.No	CommandName	Description	Type and Description
1	save	Save ipv6 w an1 configuration changes.	
2	cancel	Roll back ipv6 w an configuration changes.	
3	exit	Save ipv6 w an1 configuration changes and current mode.	

4	isp_type	Set ISP Type	ISP Types.
5	dhcpc	Set DHCPC Configurations	
6	dhcpc stateless_mode_enable	Set Stateless Mode	stateless mode configuration.
7	dhcpc prefix_delegation_enable	Enable prefix delegation	Boolean choice
8	static	set ipv6 address	
9	static ip_address	set ipv6 address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
10	static prefix	set prefix length	Unsigned integer
11	static gateway_address	Set ipv6 gateway address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
12	static primary_dns	Set ipv6 primary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
13	static secondary_dns	Set ipv6 secondary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
14	pppoe	pppoe over ipv6 configuration parameters	
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 dhcipv6_opt	Enter the dhcipv6 option for configuring additional parameters.	WAN interface type
19	pppoe primary_dns	Valid primary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
20	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]

8.37 net wan wan2 ipv6 configure

S.No	CommandName	Description	Type and Description
1	save	Save ipv6 wan2 configuration changes.	
2	cancel	Roll back ipv6 wan2 configuration changes.	
3	exit	Save ipv6 wan2 configuration changes and current mode.	
4	isp_type	Set ISP Type	ISP Types.

5	dhcpc	Set DHCPC Configurations	
6	dhcpc stateless_mode_enable	Set Stateless Mode	stateless mode configuration.
7	dhcpc prefix_delegation_enable	Enable prefix delegation	Boolean choice
8	static	set ipv6 address	
9	static ip_address	set ipv6 address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
10	static prefix	set prefix length	Unsigned integer
11	static gateway_address	Set ipv6 gateway address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
12	static primary_dns	Set ipv6 primary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
13	static secondary_dns	Set ipv6 secondary dns address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
14	pppoe	pppoe over ipv6 configuration parameters	
15	pppoe username	Enter the username to authenticate	String
16	pppoe password	Enter the password to authenticate	String
17	pppoe authOpt	Enter the Auth Option to authenticate	PPPOE Authentication Types.
18	pppoe dhcpv6_opt	Enter the dhcpv6 option for configuring additional parameters.	WAN interface type
19	pppoe primary_dns	Valid primary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
20	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]

8.38 net routing ospfv2 configure <ltinterface>

S.No	CommandName	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 become 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 device'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 Simple then ospf packets are authenticated using simple text key. If Authentication Type is MD5 then the interface authenticates ospf packets with MD5 authentication.	OSPF Authentication type
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

8.39 net routing ospfv3 configure <ltinterface>

S.No	CommandName	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 device'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

8.40 net port management configure <!tportName>

S.No	Command Name	Description	Type and Description
1	<!tportName>	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

8.41 net wan 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	Passw ord	Set Passw ord	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 w here each part is in the range 0-255
13	NetMask	Set subnet mask	IP address AAA.BBB.CCC.DDD w here 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 w here each part is in the range 0-255
16	SecondaryDns	Set Secondary DNS	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

8.42 net routing protocol_binding add

S.No	CommandName	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_Gatew ay	local gatew ay type	WAN interface type
6	Source_Netw ork	source netw ork type	firew all rule address type
7	Destination_Netw ork	destination netw ork type	firew all rule address type
8	source_address_start	starting IP of the Source Netw ork	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
9	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
10	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
11	destination_address_end	ending IP of the Destiation user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

8.43 net routing protocol_binding edit <ltrow_id>

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

8.44 net routing protocol_binding enable <ltrow_id>

S.No	CommandName	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	WAN interface type
7	Source_Network	source network type	firewall rule address type
8	Destination_Network	destination network type	firewall rule address type
9	source_address_start	starting IP of the Source Network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12	destination_address_end	ending IP of the Destination user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
----	-------------------------	-----------------------------------	---

8.45 net routing protocol_binding disable <ltrow_id>

S.No	CommandName	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_Gatew ay	local gatew ay type	WAN interface type
7	Source_Netw ork	source netw ork type	firew all rule address type
8	Destination_Netw ork	destination netw ork type	firew all rule address type
9	source_address_start	starting IP of the Source Netw ork	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
10	source_address_end	ending IP of the Source user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
11	destination_address_start	start IP of the Destination user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
12	destination_address_end	ending IP of the Destination user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255

8.46 net routing protocol_binding delete <ltrow_id>

S.No	CommandName	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_Gatew ay	local gatew ay type	WAN interface type
7	Source_Netw ork	source netw ork 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 Destination user	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

8.47 net radvd configure

S.No	CommandName	Description	Type and Description
1	save	Save radvd configuration changes.	
2	exit	Save radvd configuration changes and exit current mode.	
3	cancel	Roll back radvd configuration changes.	
4	enable	enable the RADVD process here to allow stateless auto configuration of the IPv6 LAN network	Boolean choice
5	mode	select N to send router advertisements (RA's) to all interfaces else Y	radvd advertisement mode type
6	interval	The time in seconds between sending unsolicited multicast RA's. The default is 30 seconds.	PPPOE idle timeout Type.
7	flags	RA Flags	
8	flags managed_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 router's RADVD process	radvd preference type
11	mtu	This is used in RA's to ensure all nodes on the network use the same MTU value in the cases where the LAN MTU is not well known. The default is 1500	mtu size
12	life_time	The lifetime in seconds of the route. The default is 3600 seconds.	Unsigned integer

8.48 net radvd pool add

S.No	CommandName	Description	Type and Description
1	save	Save radvd Pool configuration changes.	
2	exit	Save radvd Pool configuration changes and exit current mode.	
3	cancel	Roll back radvd Pool configuration	

		changes.	
4	prefix_type	Option whether to select the prefix type as 6to4 or Global/Local/ISATAP	ipv6 prefix type
5	sla_id	The SLA ID (Site-Level Aggregation Identifier) in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent	Unsigned integer
6	prefix_address	It specifies the IPv6 network address	String
7	prefix_length	The prefix length variable is a decimal value that indicates the number of contiguous, higher order bits of the address that make up the network portion of the address	Unsigned integer
8	prefix_life_time	The length of time over which the requesting router is allowed to use the prefix	Unsigned integer

8.49 net radvd pool edit <ltrow_id>

S.No	CommandName	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 whether to select the prefix type as 6to4 or Global/Local/ISATAP	ipv6 prefix type
6	sla_id	The SLA ID (Site-Level Aggregation Identifier) in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent	Unsigned integer
7	prefix_address	It specifies the IPv6 network address	String
8	prefix_length	The prefix length variable is a decimal value that indicates the number of contiguous, higher order bits of the address that make up the network portion of the address	Unsigned integer
9	prefix_life_time	The length of time over which the requesting router is allowed to use the prefix	Unsigned integer

8.50 net radvd pool delete <ltrow_id>

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

8.51 net routing dynamic configure

S.No	CommandName	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_frommonth	month in w hich md5 authentication key validity starts	Month in the format MM(01-12)
12	first_key valid_fromday	day in w hich md5 authentication key validity starts	Day in the format DD(01-31)
13	first_key valid_fromyear	year in w hich md5 authentication key validity starts	Year
14	first_key valid_fromhour	hour in w hich md5 authentication key validity starts	HH(00-23) using 24 hour clock
15	first_key valid_fromminute	minute in w hich md5 authentication key validity starts	minute in the format MM(00-59)
16	first_key valid_fromsecond	second in w hich 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 w hich md5 authentication key validity ends	Month in the format MM(01-12)
19	first_key valid_to day	day in w hich md5 authentication key validity ends	Day in the format DD(01-31)
20	first_key valid_to year	year in w hich md5 authentication key validity ends	Year
21	first_key valid_to hour	hour in w hich md5 authentication key validity ends	HH(00-23) using 24 hour clock
22	first_key valid_to minute	minute in w hich md5 authentication key validity ends	minute in the format MM(00-59)
23	first_key valid_to second	second in w hich 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_frommonth	month in w hich md5 authentication key validity starts	Month in the format MM(01-12)
30	second_key valid_fromday	day in w hich md5 authentication key validity starts	Day in the format DD(01-31)
31	second_key valid_fromyear	year in w hich md5 authentication key validity starts	Year
32	second_key valid_fromhour	hour in w hich md5 authentication key validity starts	HH(00-23) using 24 hour clock
33	second_key valid_fromminute	minute in w hich md5 authentication key	

		validity starts	minute in the format MM(00-59)
34	second_key valid_fromsecond	second in w hich md5 authentication key validity starts	Second in the format SS(00-59)
35	second_key valid_to month	month in w hich md5 authentication key validity ends	Month in the format MM(01-12)
36	second_key valid_to day	day in w hich md5 authentication key validity ends	Day in the format DD(01-31)
37	second_key valid_to year	year in w hich md5 authentication key validity ends	Year
38	second_key valid_to hour	hour in w hich md5 authentication key validity ends	HH(00-23) using 24 hour clock
39	second_key valid_to minute	minute in w hich md5 authentication key validity ends	minute in the format MM(00-59)
40	second_key valid_to second	second in w hich md5 authentication key validity ends	Second in the format SS(00-59)

8.52 net routing static ipv4 configure <lname>

S.No	CommandName	Description	Type and Description
1	<lname>	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 w here each part is in the range 0-255
6	subnet_mask	Set the subnet for this rule.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
7	gateway_address	Set the gateway IP.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
8	interface	Set the interface for which the rule applies.	WAN interface type
9	metric	Set the metric for this route.	Unsigned integer
10	private_flag	Defines w hether the route can be shared w ith other gatew ays when RIP is enabled	Boolean choice
11	active_flag	Defines w hether its an active route	Boolean choice

8.53 net routing static ipv6 configure <lname>

S.No	CommandName	Description	Type and Description
1	<lname>	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 where each part is in the range [0-9A-Fa-f:]
6	prefix	Set the prefix length for this rule.	Unsigned integer
7	gateway_address	Set the gateway IPV6.	IP address abcd:abcd:abcd:abcd:abcd: abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
8	interface	Set the interface for which the rule applies.	select the ipv6 interface type
9	metric	Set the metric for this route.	Unsigned integer
10	active_flag	Defines whether its an active IPV6 route	Boolean choice

8.54 net routing static ipv4 delete <lname>

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

8.55 net routing static ipv6 delete <lname>

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

8.56 net tahi add-default-route <tip_address>

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

8.57 net tahi add-route <tip_address> <lgw>

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

			in the range [0-9A-Fa-f:]
--	--	--	---------------------------

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

S.No	CommandName	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:]

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

S.No	CommandName	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:]

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

S.No	CommandName	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:]

8.61 net tahi ipv6-Alias-Add(WAN) <ltip6_address>

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

8.62 net tahi ipv6-Alias-Del(WAN) <ltip6_address>

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

8.63 net tahi reachable-time <lttime>

S.No	CommandName	Description	Type and Description
1	<lttime>	set the reachable time of neighbour cache entries	number in range of 30 to 150

8.64 net tahi ping6 <ltip> <ltsize>

S.No	CommandName	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

8.65 net tahi mping6 <ltmip>

S.No	CommandName	Description	Type and Description
1	<ltmip>	multicast ping6	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd w here each part is in the range [0-9A-Fa-f:]

8.66 net tahi pmtu-route-add <ltipAdd>

S.No	CommandName	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:]

8.67 net upnp configure

S.No	CommandName	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 9. Configuration commands under branch SECURITY

9.1 security advanced_network attack_checks configure

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

9.2 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

9.3 security advanced_network igmp allowedsubnets add

S.No	Command Name	Description	Type and Description
1	save	Save muticast source subnet configuration	
2	exit	Save igmp configuration changes and exit current mode.	
3	cancel	Roll back igmp configuration changes.	
4	multicast_source_address	Enter the address of the multicast source	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
5	multicast_source_masklength	Enter the masklength of the multicast source address	number in range of 1 to 32

9.4 security advanced_network igmp allowedsubnets edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	Edit netw ork address and mask length of multicast source	Unsigned integer
2	save	Save muticast source subnet configuration	
3	exit	Save igmp configuration changes and exit current mode.	
4	cancel	Roll back igmp configuration changes.	
5	multicast_source_address	Enter the address of the multicast source	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
6	multicast_source_masklength	Enter the masklength of the multicast source address	number in range of 1 to 32

9.5 security advanced_network igmp allowedsubnets delete <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	delete netw ork address and masklength of multicast source	Unsigned integer

9.6 security advanced_network ips setup

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

8	ips_check_active dmz-wan	Enable or Disable ips checks active between DMZ and WAN	Boolean choice
---	--------------------------	---	----------------

9.7 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

9.8 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

9.9 security application_rules delete <ltrow_id>

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

9.10 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 customservices 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 customservice.
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

9.11 security firewall custom_service edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	customservices 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 customservices 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 customservice.
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

9.12 security firewall custom_service delete <ltrow_id>

S.No	Command Name	Description	Type and Description
------	--------------	-------------	----------------------

1	</trow_id>	customservices configuration mode.	Unsigned integer
---	------------	------------------------------------	------------------

9.13 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 fromZone 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	firew all rule type
7	to_zone_vlan	Set To Zone VLAN using corresponding VLAN name	String
8	service	.	
9	service service_custom	Name of the customservice for which a rule is to be added custom name should already be added into customservice	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	firew all rule action type
12	schedule	Name of schedule for w hich the rule is applicable	String
13	source_address_type	Type of the source user	firew all rule address type
14	destination_address_type	Type of the destination user	firew all rule address type
15	snat_address_type	Type of the SNAT address	firew all rule snat address type
16	log	Log Alw ays or Never	firew all rule log enable/disable
17	source_address_start	IP of the Source user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
18	source_address_end	IP of the Source user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
19	destination_address_start	IP of the Destination user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
20	destination_address_end	IP of the Destiation user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
21	qos_priority	Firew all type of service	firew all type of service
22	w an_interface	WAN interface for Source NAT settings	WAN interface type
23	snat_address	IP of the SNAT Address	IP address AAA.BBB.CCC.DDD w here 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 WAN	WAN interface type

9.14 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

9.15 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 fromZone 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 w here each part is in the range 0-255
20	destination_address_start	IP of the Destination user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
21	destination_address_end	IP of the Destination user	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
22	qos_priority	Firew all type of service	firew all type of service
23	wan_interface	WAN interface for Source NAT settings	WAN interface type
24	snat_address	IP of the SNAT Address	IP address AAA.BBB.CCC.DDD w here 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 firew all 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 w hich is hosting the server.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
28	dnat_ipaddress	Set it as Dedicated/configured WAN	WAN interface type

9.16 security firewall ipv4 enable <ltrow_id>

S.No	CommandName	Description	Type and Description
1	<ltrow_id>	Firew all IPV4 rules configuration mode.	Unsigned integer

9.17 security firewall ipv4 disable <ltrow_id>

S.No	CommandName	Description	Type and Description
1	<ltrow_id>	Firew all IPV4 Rules configuration mode.	Unsigned integer

9.18 security firewall ipv4 delete <ltrow_id>

S.No	CommandName	Description	Type and Description
1	<ltrow_id>	Firew all IPV4 Rules configuration mode.	Unsigned integer

9.19 security firewall ipv4 move <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	Firew all IPV4 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 IPV4 rule reordering changes.	

3	exit	Save Firew all 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

9.20 security firewall algs

S.No	Command Name	Description	Type and Description
1	save	Save Firew all algs changes.	
2	exit	Save Firew all algs changes and exit current mode.	
3	cancel	Roll Firew all 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

9.21 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 customservice for w hich a rule is to be added customname should already be added into customservice	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 where each part is in the range [0-9A-Fa-f:]
14	source_end_address	IP of the Source user	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
15	source_address_prefix	prefix length of the Source user	String
16	destination_start_address	IP of the Destination user	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
17	destination_end_address	IP of the Destination user	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
18	destination_address_prefix	Prefix Length of the Destination user	String

9.22 security firewall ipv6 edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	Firew all IPV6 rules configuration mode.	Unsigned integer
2	save	Save Firew all IPV6 rules configuration changes.	
3	exit	Save Firew all 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	firew all rule type
6	service	.	
7	service service_custom	Name of the customservice for w hich a rule is to be added customname should already be added into customservice	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	firew all rule action type
10	schedule	Schedule for w hich the rule is applicable	String
11	source_address_type	Type of the source user	firew all rule address type
12	destination_address_type	Type of the destination user	firew all rule address type
13	log	Log Alw ays or Never	firew all 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 where each part is in the range [0-9A-Fa-f:]
18	destination_end_address	IP of the Destination user	IP address abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
19	destination_address_prefix	Prefix Length of the Destination user	String

9.23 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

9.24 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

9.25 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

9.26 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

9.27 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

9.28 security ids configure

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

9.29 security session_settings configure

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

9.30 security schedules add

S.No	Command Name	Description	Type and Description
1	save	Save schedules configuration changes.	
2	exit	Save schedules configuration changes and exit current mode.	
3	cancel	Roll back schedules configuration changes.	
4	name	Name of the schedule for which a rule is to be added	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.

9.31 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 which 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 wednesday	select all days for schedule days	Boolean choice
11	days thursday	select all days for schedule days	Boolean choice
12	days friday	select all days for schedule days	Boolean choice
13	days saturday	select all days for schedule days	Boolean choice
14	days sunday	select all days for schedule days	Boolean choice
15	time_of_day	scheduled time of day	
16	time_of_day all_enable	type of schedule activation for time of the day	Boolean choice
17	time_of_day start	start time	
18	time_of_day start mins	minutes	minute in the format MM(00-59)
19	time_of_day start hours	hours	schedule time unit type.
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.

9.32 security schedules delete <ltrow_id>

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

9.33 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

9.34 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

9.35 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

9.36 security mac_filter source delete <ltrow_id>

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

9.37 security ip_or_mac_binding add

S.No	CommandName	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 where each part is in the range 0-255
7	log_dropped_packets	Specify logging option for this rule	Boolean choice

9.38 security ip_or_mac_binding edit <ltrow_id>

S.No	CommandName	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 which policies will be applied	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
7	ip_address	enter ip address to which policies will be applied	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	log_dropped_packets	Specify logging option for this rule	Boolean choice

9.39 security ip_or_mac_binding delete <ltrow_id>

S.No	CommandName	Description	Type and Description
------	-------------	-------------	----------------------

1	<ltrow_id>	ip/mac binding configuration mode.	Unsigned integer
---	------------	------------------------------------	------------------

9.40 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

9.41 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

9.42 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

9.43 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

9.44 security website_filter approved_urls delete <ltrow_id>

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

9.45 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

9.46 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

9.47 security website_filter blocked_keywords delete <ltrow_id>

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

9.48 security website_filter blocked_keywords enable <ltrow_id>

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

9.49 security website_filter blocked_keywords disable <ltrow_id>

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

Chapter 10. Configuration commands under branch SYSTEM

10.1 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_wan_accept_packet_logs	lan to wan accepted Pkts Enable/Disable	Boolean choice
5	lan_wan_drop_packet_logs	lan to wan dropped Pkts Enable/Disable	Boolean choice
6	wan_lan_accept_packet_logs	wan to lan accepted Pkts logs Enable/Disable	Boolean choice
7	wan_lan_drop_packet_logs	wan to lan dropped Pkts logs Enable/Disable	Boolean choice
8	wan_dmz_accept_packet_logs	wan to dmz accepted Pkts logs Enable/Disable	Boolean choice
9	wan_dmz_drop_packet_logs	wan to dmz dropped Pkts logs Enable/Disable	Boolean choice
10	dmz_wan_accept_packet_logs	dmz to wan accepted Pkts logs Enable/Disable	Boolean choice
11	dmz_wan_drop_packet_logs	dmz to wan dropped Pkts logs Enable/Disable	Boolean choice
12	dmz_lan_accept_packet_logs	dmz to lan accepted Pkts logs Enable/Disable	Boolean choice
13	dmz_lan_drop_packet_logs	dmz to lan dropped Pkts logs Enable/Disable	Boolean choice
14	lan_dmz_accept_packet_logs	lan to dmz accepted Pkts logs Enable/Disable	Boolean choice
15	lan_dmz_drop_packet_logs	lan to dmz dropped Pkts logs Enable/Disable	Boolean choice
16	unicast_traffic_logs	All Unicast Traffic logs Enable/Disable	Boolean choice
17	broadcast_or_multicast_traffic_logs	All Broadcast/Multicast Traffic logs Enable/Disable	Boolean choice
18	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

10.2 system logging facility configure

<ltfacility>

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

10.3 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 whether 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 where logs and alerts will 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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 w here 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

10.4 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_w an_accept_enable	Enable/Disable logging for the LAN to WAN Accept packets	Boolean choice
5	lan_w an_drop_enable	Enable/Disable logging for the LAN to WAN Dropped packets	Boolean choice
6	w an_lan_accept_enable	Enable/Disable logging for the WAN to LAN Accept packets	Boolean choice
7	w an_lan_drop_enable	Enable/Disable logging for the WAN to LAN Dropped packets	Boolean choice

10.5 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 w here 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 w here 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

10.6 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 w here 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 w here each part is in the range 0-255

10.7 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 w here 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 w here 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 w ill be sent to.	Port number
8	community	The community string to w hich the agent belongs. Most agents are configured to listen for traps in the Public community	String

10.8 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 w here each part is in the range 0-255

10.9 system snmp users configure <ltuser>

S.No	Command Name	Description	Type and Description
1	<ltuser>	SNMP v3 User list configuration changes	snmpv3users list user type
2	save	Save SNMP trap configuration changes.	

3	exit	save SNMP v3 Users configuration changes and exit current mode.	
4	cancel	Roll back SNMP v3 Users configuration changes.	
5	security_level	authentication and privacy settings .	snmp security level type for snmpv3users list
6	authentication_algo	choose betw een 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 passw ord with the SNMPv3 user.	String
9	privacy_password	shared privacy passw ord with the SNMPv3 user	String

10.10 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

10.11 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 w here 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 w here 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

10.12 system snmp access edit <ltrowid>

S.No	Command Name	Description	Type and Description
1	<ltrowid>	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 manage 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

10.13 system snmp access delete </trowid>

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

10.14 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 power mode configuration changes.	
4	link_status	Enable/Disable Link status	Boolean choice
5	cable_length	enable/disable Cable Length	Boolean choice

10.15 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

10.16 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 ntp 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

10.17 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(Dow nload 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

10.18 system usb usb1 configure

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

10.19 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 WAN settings changes.	
4	enable	Enable USB2	Boolean choice
5	printer_enable	Enable printer	Boolean choice
6	Storage_enable	Enable USB2	Boolean choice
7	usb_type	Select the USB type 3G_USB_ADAPTOR/USB_Disc	usb device type

10.20 system usb shareport_vlan configure <ltrow_id>

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

10.21 system groups configure

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

10.22 system group add

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

10.23 system group edit <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	systemgroups edit mode.	Unsigned integer
2	save	Save systemgroup configuration changes.	
3	exit	Save systemgroup configuration changes and exit current mode.	
4	cancel	Roll back systemgroup 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

10.24 system group delete <ltrow_id>

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

10.25 system users add

S.No	Command Name	Description	Type and Description
1	save	Save systemuser configuration changes.	
2	exit	Save systemuser configuration changes and exit current mode.	
3	cancel	Roll back systemuser 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 passw ord here	String
8	password_confirm	Re-Enter the passw ord here	String
9	groupname	Enter the groupname here	String
10	usertimeout	Enter the time out for group	Unsigned integer

10.26 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 passw ord here	String
9	password_confirm	Re-Enter the passw ord here	String
10	groupname	Enter the groupname here	String
11	usertimeout	Enter the time out for group	Unsigned integer

10.27 system users delete <ltrow_id>

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

10.28 system users password <ltuser>

S.No	Command Name	Description	Type and Description
1	<ltuser>	Change passw ord.	String

10.29 system users idle_timeout <lttimeout>

S.No	Command Name	Description	Type and Description
1	<lttimeout>	Change idle timeout.	Unsigned integer

10.30 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_wan	deny login wan	Boolean choice
11	allow_login_from_defined_ips	login from ip	Boolean choice
12	allow_login_from_defined_browsers	login from browser	Boolean choice

10.31 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

10.32 system group access_control_browser delete <ltrow_id>

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

10.33 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 w here each part is in the range 0-255
7	mask_length	Set the source network mask length	number in range of 1 to 32

10.34 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 11. Configuration commands under branch DOT11

11.1 dot11 profile add <ltprofile_name>

S.No	Command Name	Description	Type and Description
1	<ltprofile_name>	802.11 profile configuration mode.	String
2	save	Save profile configuration changes	
3	exit	Save profile configuration changes and exit current mode.	
4	ssid	Set the 802.11 profile SSID.	String
5	broadcast-ssid	Enable or disable SSID broadcast.	Boolean choice
6	security_type	Set the profile security type.	802.11 Security Types
7	w ep	Set profile WEP options.	
8	w ep authentication	Set WEP authentication type.	WEP Authentication Types
9	w ep encryption	Set WEP encryption type.	WEP Encryption Types
10	w ep key	Set WEP key. Not required if passphrase is set.	WEP key index type (1-4) String
11	w ep passphrase	Set WEP passphrase to generate WEP key from.	WEP key index type (1-4) String
12	w pa	Set the WPA options.	
13	w pa authentication	Set WPA authentication type.	WPA Authentication Types
14	w pa encryption	Set WPA encryption type.	WPA Encryption Types
15	w pa wpa-password	WPA Passw ord. Needed only if authentication is PSK	String

11.2 dot11 profile edit <ltprofile_name>

S.No	Command Name	Description	Type and Description
1	<ltprofile_name>	802.11 profile configuration mode.	String
2	save	Save profile configuration changes	
3	exit	Save profile configuration changes and exit current mode.	
4	ssid	Set the 802.11 profile SSID.	String
5	broadcast-ssid	Enable or disable SSID broadcast.	Boolean choice
6	security_type	Set the profile security type.	802.11 Security Types
7	w ep	Set profile WEP options.	
8	w ep authentication	Set WEP authentication type.	WEP Authentication Types
9	w ep encryption	Set WEP encryption type.	WEP Encryption Types
10	w ep key	Set WEP key. Not required if passphrase is set.	

			WEP key index type (1-4) String
11	w ep passphrase	Set WEP passphrase to generate WEP key from.	WEP key index type (1-4) String
12	w pa	Set the WPA options.	
13	w pa authentication	Set WPA authentication type.	WPA Authentication Types
14	w pa encryption	Set WPA encryption type.	WPA Encryption Types
15	w pa wpa-password	WPA Passw ord. Needed only if authentication is PSK	String

11.3 dot11 radius configure

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

11.4 dot11 profile delete <ltprofile_name>

S.No	Command Name	Description	Type and Description
1	<ltprofile_name>	Delete an 802.11 profile.	String

11.5 dot11 accesspoint configure <ltap_name>

S.No	Command Name	Description	Type and Description
1	<ltap_name>	802.11 access point configuration mode	String
2	save	Save AP configuration changes	
3	cancel	Roll back AP configuration changes	
4	exit	Save AP configuration changes and exit current mode.	
5	profile	Set the 802.11 profile the AP w ill use.	String
6	w lan_partition	Enable or Disable w lan_partition.	Boolean choice
7	enable_active_time	Setting time.	Boolean choice
8	start	Setting the time limits.	
9	stop	Setting the time limits.	

10	start hour	Setting the time limits.	H(1-12) using 12 hour clock
11	stop hour	Setting the time limits.	H(1-12) using 12 hour clock
12	start minute	Setting the time limits.	minute in the format MM(00-59)
13	stop minute	Setting the time limits.	minute in the format MM(00-59)
14	start meridian	Setting the time limits.	Schedule Meridien Types.
15	stop meridian	Setting the time limits.	Schedule Meridien Types.

11.6 dot11 accesspoint delete <ltap_name>

S.No	Command Name	Description	Type and Description
1	<ltap_name>	Delete an 802.11 access point.	String

11.7 dot11 accesspoint disable <ltap_name>

S.No	Command Name	Description	Type and Description
1	<ltap_name>	Disable an 802.11 access point.	String

11.8 dot11 accesspoint enable <ltap_name>

S.No	Command Name	Description	Type and Description
1	<ltap_name>	Enable an 802.11 access point.	String

11.9 dot11 radio configure

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

11.10 dot11 radio advanced configure

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

11.11 dot11 accesspoint wps configure

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

11.12 dot11 accesspoint ACL configure <ltap_name>

S.No	Command Name	Description	Type and Description
1	<ltap_name>	802.11 AP ACL configuration mode.	String
2	save	Save AP ACL configuration changes.	
3	cancel	Roll back AP ACL configuration changes	
4	exit	Save AP ACL configuration changes and exit current mode.	
5	acl_policy	Set accesspoint ACL Policy.	

			Accesspoint ACL Policy type
6	mac_address	Set accesspoint mac address.	MAC address AA:BB:CC:DD:EE:FF w here each part is in the range 00-FF

11.13 dot11 accesspoint acl delete_mac_address <ltrowid>

S.No	Command Name	Description	Type and Description
1	<ltrowid>	Delete acl mac address entry.	Unsigned integer

Chapter 12. Configuration commands under branch VPN

12.1 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_v4	enable/disable L2TP server in IPv4 mode only.	Boolean choice
5	enable_v6	enable/disable L2TP server in IPv4/IPv6 mode.	Boolean choice
6	Natenable	enable/disable L2TP NAT routing mode	Boolean choice
7	start_address	L2TP server starting IP address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
8	end_address	L2TP server ending IP address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
9	ipv6_prefix	L2TP server IPv6 Prefix	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
10	EnablePap	enable pap authentication	Boolean choice
11	EnableChap	enable chap authentication	Boolean choice
12	EnableMSChapChap	enable MSChap authentication	Boolean choice
13	MSChapv2Enable	enable MSChapv2Enable authentication	Boolean choice
14	l2tpSecretKeyEnable	L2TP Enanle secret key	Boolean choice
15	secretKey	L2TP secret Key	String
16	timeout	User Time Out	Unsigned integer

12.2 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 w here each part is in the range 0-255
6	remote_network	Remote Network Address	IP address AAA.BBB.CCC.DDD w here 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

12.3 vpn pptp client_action </taction>

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

12.4 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_v4	enable/disable PPTP server in IPv4 mode only.	Boolean choice
5	enable_v6	enable/disable PPTP server in IPv4/IPv6 mode.	Boolean choice
6	Natenable	enable/disable PPTP NAT routing mode	Boolean choice
7	start_address	PPTP server starting IP address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
8	end_address	PPTP server ending IP address.	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
9	ipv6_prefix	PPTP server IPv6 Prefix	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
10	pap_enable	PPTP server PAP authentication	Boolean choice
11	chap_enable	PPTP server CHAP authentication	Boolean choice
12	mschap_enable	PPTP server MSCHAP authentication	Boolean choice
13	mschapv2_enable	PPTP server MSCHAPV2 authentication	Boolean choice
14	Mppe40Enable	PPTP server Mppe40	Boolean choice
15	Mppe128Enable	PPTP server Mppe128	Boolean choice
16	MppeStatefulEnable	PPTP server MppeStateful	Boolean choice
17	UserTimeOut	PPTP server User TimeOut	Unsigned integer

12.5 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 w hether the banner message should be displayed	Boolean choice
9	enable_httpmetatags	Specify w hether the http meta tags should be enabled	Boolean choice
10	enable_activexwebcache cleaner	Specify w hether the activex web cache cleaner should be enabled	Boolean choice
11	enable_vpntunnel	Specify w hether the vpn tunnel should be enabled	Boolean choice
12	enable_portforwarding	Specify w hether the port forwarding should be enabled	Boolean choice

12.6 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 w hether the banner message should be displayed	Boolean choice
10	enable_httpmetatags	Specify w hether the http meta tags should be enabled	Boolean choice
11	enable_activexwebcache cleaner	Specify w hether the activex web cache cleaner should be enabled	Boolean choice
12	enable_vpntunnel	Specify w hether the vpn tunnel should be enabled	Boolean choice
13	enable_portforwarding	Specify w hether the port forwarding should be enabled	Boolean choice

12.7 vpn sslvpn portal-layouts delete <ltrow_id>

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

12.8 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

12.9 vpn sslvpn portforwarding appconfig add

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

12.10 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

12.11 vpn sslvpn portforwarding hostconfig add

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

12.12 vpn sslvpn portforwarding hostconfig delete <ltrow_id>

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

12.13 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

12.14 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 AAA.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

12.15 vpn sslvpn resource configure delete <ltrow_id>

S.No	CommandName	Description	Type and Description
------	-------------	-------------	----------------------

1	<ltrow_id>	Delete an sslvpn resource object	Unsigned integer
---	------------	----------------------------------	------------------

12.16 vpn sslvpn resource delete <ltrow_id>

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

12.17 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_ow ner	policy ow ner	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 w here 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

12.18 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_ow ner	policy ow ner	

			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 w here 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

12.19 vpn sslvpn policy delete </trow_id>

S.No	CommandName	Description	Type and Description
1	</trow_id>	Delete an sslvpn policy	Unsigned integer

12.20 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

12.21 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 network	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

12.22 vpn sslvpn route delete <ltrow_id>

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

12.23 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_server1	Specify the authentication server	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
8	authentication_server2	Specify the authentication server	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
9	authentication_server3	Specify the authentication server	IP address AAA.BBB.CCC.DDD w here 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_secret2	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_dn	Specify the ldap base domain name	String
18	active_directory_domain	Specify the active directory domain	String
19	second_active_directory_domain	Specify the active directory domain	String

12.24 vpn sslvpn users domains edit <ldomain_Name>

S.No	Command Name	Description	Type and Description
1	<ldomain_Name>	Users domain configuration mode	String
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 w here each part is in the range 0-255
9	authentication_server2	Specify the authentication server	IP address AAA.BBB.CCC.DDD w here each part is in the range 0-255
10	authentication_server3	Specify the authentication server	IP address AAA.BBB.CCC.DDD w here 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	w orkgroup	Specify the w ork group	String
16	second_workgroup	Specify the w ork 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

12.25 vpn sslvpn users domains delete <ltomainname>

S.No	Command Name	Description	Type and Description
1	<ltomainname>	Users domain delete mode	String

12.26 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.

12.27 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.

12.28 vpn sslvpn users groups delete <ltrow_id>

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

12.29 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	confirm the user's password	String
11	idle_timeout	Enter the user's timeout value	idle timeout value for user.

12.30 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	confirm the user's password	String
12	idle_timeout	Enter the user's timeout value	idle timeout value for user.

12.31 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_wan_interface	enable/disable login from wan	Boolean choice

12.32 vpn sslvpn users users browser_policies <ltrow_id>

S.No	Command Name	Description	Type and Description
1	<ltrow_id>	Users browser 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

12.33 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

12.34 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

12.35 vpn sslvpn users users delete <ltrow_id>

S.No	CommandName	Description	Type and Description
1	<ltrow_id>	Users delete mode	Unsigned integer

12.36 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 ipv4 or ipv6	vpn protocol version
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.	IPV4 or IPV6 address depending upon protocol selected IPV4 or IPV6
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	IPV4 or IPV6 address depending upon protocol selected IPV4 or IPV6
21	general_local_end_address	IP address where the range needs to end	IPV4 or IPV6 address

			depending upon protocol selected IPV4 or IPV6
22	general_local_subnet_mask	Subnet mask of the subnet used	IP address AAA.BBB.CCC.DDD w here 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	IPV4 or IPV6 address depending upon protocol selected IPV4 or IPV6
26	general_remote_end_address	IP address where the range needs to end	IPV4 or IPV6 address depending upon protocol selected IPV4 or IPV6
27	general_remote_subnet_mask	Subnet mask of the subnet used	IP address AAA.BBB.CCC.DDD w here 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	IPV4 or IPV6 address depending upon protocol selected IPV4 or IPV6
31	general_keepalive_destinationip	keepalive destinationip	IPV4 or IPV6 address depending upon protocol selected IPV4 or IPV6
32	general_keepalive_detection_period	keepalive detection period	keepalive detection period in seconds
33	general_keepalive_failure_count	keepalive failure count	keepalive failure count
34	manual_spi_in	Takes a hexadecimal value between 3 and 8 characters.	Takes a hexadecimal value between 3 and 8 characters
35	manual_spi_out	Takes a hexadecimal value between 3 and 8 characters.	Takes a hexadecimal value between 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 with 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 with 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_frequency	Setting IKE nat alive frequency	Unsigned integer
46	auto_phase1_local_identytype	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_identytype	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	
52	auto_phase1_encryption_algorithmDES	Setting IKE encryption algorithm	
53	auto_phase1_encryption_algorithmDES enable_DES	Enable DES encryption algorithm	Boolean choice
54	auto_phase1_encryption_algorithm3DES	Setting IKE encryption algorithm	
55	auto_phase1_encryption_algorithm3DES enable_3DES	Enable 3DES encryption algorithm	Boolean choice
56	auto_phase1_encryption_algorithmAES-128	Setting IKE encryption algorithm	
57	auto_phase1_encryption_algorithmAES-128 enable_AES-128	Enable AES-128 encryption algorithm	Boolean choice
58	auto_phase1_encryption_algorithmAES-192	Setting IKE encryption algorithm	
59	auto_phase1_encryption_algorithmAES-192 enable_AES-192	Enable AES-192 encryption algorithm	Boolean choice
60	auto_phase1_encryption_algorithmAES-256	Setting IKE encryption algorithm	
61	auto_phase1_encryption_algorithmAES-256 enable_AES-256	Enable AES-256 encryption algorithm	Boolean choice
62	auto_phase1_encryption_algorithmBLOWFISH	Setting IKE encryption algorithm	
63	auto_phase1_encryption_algorithmBLOWFISH enable_BLOWFISH	Enable BLOWFISH encryption algorithm	Boolean choice
64	auto_phase1_encryption_algorithmBLOWFISH keylength	Enter BLOWFISH keylength	Unsigned integer
65	auto_phase1_encryption_algorithmCAST128	Setting IKE encryption algorithm	
66	auto_phase1_encryption_algorithmCAST128 enable_CAST128	Enable CAST128 encryption algorithm	Boolean choice
67	auto_phase1_encryption_algorithmCAST128 keylength	Enter CAST128 keylength	Unsigned integer
68	auto_phase1_auth_algorithm	Setting IKE authentication algorithm	
69	auto_phase1_auth_algorithmMD5	Setting IKE authentication algorithm	
70	auto_phase1_auth_algorithmMD5 enable_MD5	Enable MD5 authentication algorithm	Boolean choice
71	auto_phase1_auth_algorithmSHA1	Setting IKE authentication algorithm	

72	auto_phase1_auth_algorithmSHA1 enable_SHA1	Enable SHA1 authentication algorithm	Boolean choice
73	auto_phase1_auth_algorithmSHA2-256	Setting IKE authentication algorithm	
74	auto_phase1_auth_algorithmSHA2-256 enable_SHA2-256	Enable SHA2-256 authentication algorithm	Boolean choice
75	auto_phase1_auth_algorithmSHA2-384	Setting IKE authentication algorithm	
76	auto_phase1_auth_algorithmSHA2-384 enable_SHA2-384	Enable SHA2-384 authentication algorithm	Boolean choice
77	auto_phase1_auth_algorithmSHA2-512	Setting IKE authentication algorithm	
78	auto_phase1_auth_algorithmSHA2-512 enable_SHA2-512	Enable SHA2-512 authentication algorithm	Boolean choice
79	auto_phase1_auth_method	Setting IKE authentication algorithm method	IPsec VPN IKE authentication algorithm method
80	auto_phase1_dh_group	Setting IKE Diffie-Hellman (DH) Group	IPsec VPN IKE Diffie-Hellman (DH) Group type
81	auto_phase1_sa_lifetime	Setting IKE SA lifetime in seconds	Unsigned integer
82	auto_phase1_pre_shared_key	Setting IKE pre shared key	String
83	auto_phase1_enable_dead_peer_detection	Enabling/Disabling dead peer detection	Boolean choice
84	auto_phase1_detection_period	Setting dead peer detection time period	Unsigned integer
85	auto_phase1_reconnect_failure_count	Setting dead peer detection failure count	Unsigned integer
86	auto_phase1_extended_authentication	setting extended authentication method	IPsec VPN IKE extended authentication method
87	auto_phase1_authentication_type	setting extended authentication type	IPsec VPN IKE extended authentication method
88	auto_phase1_xauth_username	Username for extended authentication	String
89	auto_phase1_xauth_password	Passw ord for extended authentication	String
90	auto_phase2_sa_lifetime	vpn auto policy phase2 configure	
91	auto_phase2_sa_lifetime seconds	Setting IKE SA lifetime in seconds	Unsigned integer
92	auto_phase2_sa_lifetime bytes	Setting IKE SA lifetime in bytes	Unsigned integer
93	auto_phase2_encryption_algorithm	Setting IKE encryption algorithm	
94	auto_phase2_encryption_algorithmDES	Setting IKE encryption algorithm	
95	auto_phase2_encryption_algorithmDES enable_DES	Enable DES encryption algorithm	Boolean choice
96	auto_phase2_encryption_algorithm3DES	Setting IKE encryption algorithm	
97	auto_phase2_encryption_algorithm3DES enable_3DES	Enable 3DES encryption algorithm	Boolean choice
98	auto_phase2_encryption_algorithmAES-128	Setting IKE encryption algorithm	
99	auto_phase2_encryption_algorithmAES-128 enable_AES-128	Enable AES-128 encryption algorithm	Boolean choice
100	auto_phase2_encryption_algorithmAES-192	Setting IKE encryption algorithm	
101	auto_phase2_encryption_algorithmAES-192 enable_AES-192	Enable AES-192 encryption algorithm	Boolean choice
102	auto_phase2_encryption_algorithmAES-256	Setting IKE encryption algorithm	
103	auto_phase2_encryption_algorithmAES-256 enable_AES-256	Enable AES-256 encryption algorithm	Boolean choice
104	auto_phase2_encryption_algorithmAES-CCM	Setting IKE encryption algorithm	

105	auto_phase2_encryption_algorithmAES-CCM enable_AES-CCM	Enable AES-CCM encryption algorithm	Boolean choice
106	auto_phase2_encryption_algorithmAES-GCM	Setting IKE encryption algorithm	
107	auto_phase2_encryption_algorithmAES-GCM enable_AES-GCM	Enable AES-GCM encryption algorithm	Boolean choice
108	auto_phase2_encryption_algorithmTWOFISH-128	Setting IKE encryption algorithm	
109	auto_phase2_encryption_algorithmTWOFISH-128 enable_TWOFISH-128	Enable TWOFISH-128 encryption algorithm	Boolean choice
110	auto_phase2_encryption_algorithmTWOFISH-192	Setting IKE encryption algorithm	
111	auto_phase2_encryption_algorithmTWOFISH-192 enable_TWOFISH-192	Enable TWOFISH-192 encryption algorithm	Boolean choice
112	auto_phase2_encryption_algorithmTWOFISH-256	Setting IKE encryption algorithm	
113	auto_phase2_encryption_algorithmTWOFISH-256 enable_TWOFISH-256	Enable TWOFISH-256 encryption algorithm	Boolean choice
114	auto_phase2_encryption_algorithm BLOWFISH	Setting IKE encryption algorithm	
115	auto_phase2_encryption_algorithm BLOWFISH enable_BLOWFISH	Enable BLOWFISH encryption algorithm	Boolean choice
116	auto_phase2_encryption_algorithm BLOWFISH keylength	Enter BLOWFISH keylength	Unsigned integer
117	auto_phase2_encryption_algorithmCAST128	Setting IKE encryption algorithm	
118	auto_phase2_encryption_algorithmCAST128 enable_CAST128	Enable CAST128 encryption algorithm	Boolean choice
119	auto_phase2_encryption_algorithmCAST128 keylength	Enter CAST128 keylength	Unsigned integer
120	auto_phase2_auth_algorithm	Setting IKE authentication algorithm	
121	auto_phase2_auth_algorithmMD5	Setting IKE authentication algorithm	
122	auto_phase2_auth_algorithmMD5 enable_MD5	Enable MD5 authentication algorithm	Boolean choice
123	auto_phase2_auth_algorithmSHA 1	Setting IKE authentication algorithm	
124	auto_phase2_auth_algorithmSHA 1 enable_SHA 1	Enable SHA1 authentication algorithm	Boolean choice
125	auto_phase2_auth_algorithmSHA2-256	Setting IKE authentication algorithm	
126	auto_phase2_auth_algorithmSHA2-256 enable_SHA2-256	Enable SHA2-256 authentication algorithm	Boolean choice
127	auto_phase2_auth_algorithmSHA2-384	Setting IKE authentication algorithm	
128	auto_phase2_auth_algorithmSHA2-384 enable_SHA2-384	Enable SHA2-384 authentication algorithm	Boolean choice
129	auto_phase2_auth_algorithmSHA2-224	Setting IKE authentication algorithm	
130	auto_phase2_auth_algorithmSHA2-224 enable_SHA2-224	Enable SHA2-224 authentication algorithm	Boolean choice
131	auto_phase2_auth_algorithmSHA2-512	Setting IKE authentication algorithm	
132	auto_phase2_auth_algorithmSHA2-512 enable_SHA2-512	Enable SHA2-512 authentication algorithm	Boolean choice
133	auto_phase2_enable_pfskeygroup	Enable/Disable PFS key group	Boolean choice
134	auto_phase2_dh_group	Setting IKE Diffie-Hellman (DH) Group	IPsec VPN IKE Diffie-Hellman (DH) Group type

12.37 vpn ipsec policy enable </ltname>

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

12.38 vpn ipsec policy disable <lname>

S.No	CommandName	Description	Type and Description
1	<lname>	disable a vpn policy	String

12.39 vpn ipsec policy delete <lname>

S.No	CommandName	Description	Type and Description
1	<lname>	delete a vpn policy	String

12.40 vpn ipsec policy connect <lname>

S.No	CommandName	Description	Type and Description
1	<lname>	connect a vpn tunnel	String

12.41 vpn ipsec policy drop <lname>

S.No	CommandName	Description	Type and Description
1	<lname>	drop a vpn tunnel	String

Chapter 13. Configuration commands under branch RADIUS

13.1 radius configure <ltradius_server>

S.No	Command Name	Description	Type and Description
1	<ltradius_server>	RADIUS configuration mode.	IP address AAA.BBB.CCC.DDD w here 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 w here 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

13.2 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 w here each part is in the range 0-255