CLI Reference Guide

Unified Services Router

D-Link Corporation

http://www.dlink.com

CLI Reference Guide
DSR-500AC/1000AC
Unified Services Router
Version 1.00

Copyright Notice

Disclaimer

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

Limitations of Liability

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

Table of Contents

Chapter 1. Introduction

This document describes the Command Line Interface (CLI) for managing D-Link's DSR-500AC/1000AC router.

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

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

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

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

1.1 Accessing the CLI

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

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

 Welcome to the DSR Command Line Interface

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

D-Link DSR>
```

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

Chapter 2. Basic commands available on the CLI

2.1 Context Sensitive Help

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

2.2 Auto-Completion

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

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

2.3 Movement Keys

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

2.4 Deletion Keys

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

2.5 Escape Sequences

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

Chapter 3. Command Hierarchy in CLI

3.1 CLI Commands

The CLI commands are divided into 4 categories:

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

3.2 Router Configuration

The router configuration is divided into 5 branches:

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

Chapter 4. Global commands used in CLI

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

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

Chapter 5. Show commands used in CLI

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

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

1	show activeDirectory-serverCheck	Displays status of Active Directory servers.

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

1	show NT-Domain-Settings	Displays NT Domain configuration.

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

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

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

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

1	show LDAP-Settings	Displays LDAP configuration.

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

1	show dot11	Displays 802.11 configuration
2	show dot11 accesspoint*<ap_name>*	Displays Access Point configuration. This command displays the list of configured Access Points for the device. From this summary list, status and parameters of each AP are available for display.

		ap_name: This is an AP identifier which uniquely identifies an AP in the list of configured APs. **Enabled:** An AP can be disabled if not in use and enabled as needed. The AP is disabled if this field has the value 'N' and it is enabled if it has the value 'Y'. Disabling an AP does not delete the configuration, but stops the AP. Enabling the AP creates a wireless network where computers and other devices can join and communicate with the devices connected to the access point or the devices on the Local Area Network (LAN). **SSID:** The name or Service Set Identifier (SSID) is the name of the wireless network serviced by this AP. Note that since a given wireless profile can be common to multiple APs, the SSID is not unique to an AP. In order for computers or devices to communicate via this wireless network serviced by this AP, all devices must select the same SSID from the list of wireless networks in the area.**Broadcast:** The field indicates whether SSID is broadcasted or not in the beacon frames transmitted by the AP. If SSID is not broadcasted, the wireless devices will not be able to see the network name (SSID). If this field has the value 'Y', it indicates that the AP's SSID is broadcasted to the public. If it is 'N' it indicates the SSID is not to be broadcasted and a device would have to specify the SSID exactly to connect to this AP. **Profile:** This field has a brief description of the security, encryption and authentication combination assigned to the AP. A Profile is not necessarily unique to an AP, rather this grouping of wireless settings can be used on more than one AP at the same time. **Radio:** The physical radio(s) on which this AP is running on. An AP can run on multiple radios at the same time for load-balancing and better throughput. **VLAN:** The AP can be a part of a logical network defined by the VLAN id. This allows devices connected to the VLAN through this AP to exchange data with one another as in a LAN. If the optional argument ap_name is specified, the following configuration information is displayed for the access point. **Beacon Interval:** The amount of time in milliseconds between beacon transmissions. **DTIM Interval:** Interval for delivery of traffic

		indication message. It is related to beacon interval. **RTS Threshold:** The Request to Send (RTS) threshold is the value the AP checks against its transmitting frames to determine if the RTS/Clear To Send (CTS) handshake is required with the receiving client. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of the network packet. The default is 2346, which effectively disables RTS. **Frag Threshold:** This is the maximum length of the frame, beyond which packets must be broken up (fragmented) into two or more frames. Collisions occur more often for long frames because sending them occupies the channel for a longer time. The default is 2346, which effectively disables Fragmentation. **Preamble Mode:** 802.11b requires that a preamble be prepended to every frame before it is transmitted to the air. The preamble may be either the traditional long preamble, which requires 192 micro second for transmission, or it may be an optional short preamble that requires only 96 micro second. Long preamble is needed for the compatibility with legacy 802.11 systems operating at 1 and 2 Mbps. The default is 'long'. **RTS/CTS Protection:** If selected the AP always performs RTS/CTS handshake before transmitting a packet. It is generally used to minimize collisions among hidden stations **Transmit Power Gain:** Defines the relative amplification (gain) in dbm for transmitted packets which is added to the TX power configured on the physical radio. **Retry Limit:** The number of retries the AP will use when a frame transmission fails. It is used for both long and short frames, of size less than or equal to the RTS threshold. **Supported Rate:** The rate or rates (in Mbps) which the AP will advertise in the beacon frames.
3	show dot11 profile*<profile_name><display_qos>*	Displays Profile configuration. If no profile name is specified, this command will display a summary of the details of all the profiles configured in the system. If a profile name is specified, this command will display a detailed configuration of the profile. If the argument 'DisplayQosInfo' is set to 'Y', the profile details will include the QoS details as well.

4	show dot11 statistics	Displays access point and radio statistics. This table shows a cumulative total of relevant wireless statistics for the APs and radios; the counter is reset when the device is rebooted. **Radio Statistics**: This table displays transmit/receive data for each radio. It has the following fields: **Pkt(Tx/Rx):** The number of transmitted/received wireless packets. **Byte(Tx/Rx):** The number of transmitted/received bytes of information. **Err(TRx/Rx):** The number of transmitted/received packet errors reported to the radio. **Drop(Tx/Rx):** The number of transmitted/received packet drops between the radio and client. **Mcast**: The number of multicast packets sent over this radio. **Coll:** The number of packet collisions reported to the radio. **AP Statistics:** This table displays transmit/receive data for each AP. An AP can have multiple entries if it is running on multiple radios. It has the following fields: Pkt(Tx/Rx): The number of transmitted/received wireless packets **Byte(Tx/Rx):** The number of transmitted/received bytes of information **Err(TRx/Rx):** The number of transmitted/received packet errors reported to the AP. **Drop(Tx/Rx):** The number of transmitted/received packet dropped by the AP. **Mcast:** The number of multicast packets sent over this AP. **Coll:** The number of packet collisions reported to the AP
5	show dot11 acl<*ap_name*>	Displays access control list information for the specified access point.
6	show dot11 accesspoint status<*ap_name*>	Displays wireless stats.
7	show dot11 wmm<*profile_name*>	Displays wireless stats.
8	show dot11 radius	Displays radius Information.
9	show dot11 wps	Displays WPS Information.
10	show dot11 wds<*radio_no*>	Displays WDS Information.
11	show dot11 wireless_statistics	Displays wireless_statistics Information.
12	show dot11 radio<*radio_no*>	Displays Radio configuration. **Available Radios** This table shows the list of available radios that an AP may use. It has the following fields: **Radio:** The radio number. **Card:** This field indicates which card the radio is using. **Path:** This field indicates which path the radio is

		mapped to. **RogueAP Enabled:** If this field has value 'Y' it indicates that RogueAP detection is enabled on this radio. If it is 'N' it indicates that RogueAP detection is disabled on this radio. If the optional argument radioNum is given, the following cofiguration information is displayed for the given radio. **Radio Settings Radio:** The radio number. **Card Name:** This field indicates which card the radio is using. **Path:** This field indicates which path the radio is mapped to. **Current Channel:** The channel used by the radio. **RogueAP Enabled:** If this field has the value 'Yes', it indicates that RogueAP detection is enabled on this radio. **TX Power:** Value in dBm is the default transmitted power level for all APs that use this radio. **RX Diversity:** Enable receive diversity (use multiple antennas to receive packets) List of Access Points for Radio This table shows all the APs that are configured for a particular radio. **AP Name:** This is the name of the AP. **BSSID:** The BSSID of the AP **SSID:** The SSID serviced by AP Profile: This field has a brief description of the security, encryption and authentication combination assigned to the AP.

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

1	show POP3-Settings	Displays POP3 configuration.

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

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

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

1	show system logging	.
2	show system logging remote	.
3	show system logging remote setup	Displays remote logging configuration
4	show system logging facility	.
5	show system logging facility setup *<facility>*	Displays logging facility configuration
6	show system logging ipv4	.

7	show system logging ipv4 setup	Displays logging configuration
8	show system logging ipv6	.
9	show system logging ipv6 setup	Displays ipv6 logs configuration
10	show system log	Displays captured log messages of the router activities
11	show system log all	Displays all the 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 system log 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 system remote_management	.
14	show system remote_management setup	Displays remote management over https configuration
15	show system sessionSettings	Displays sessionSettings Configuration
16	show system snmp *<agentIP>*	Displays SNMP configuration
17	show system switch_setting	.
18	show system switch_setting power_mode	Displays power mode configuration
19	show system switch_setting jumbo_frame	Displays jumbo frame configuration
20	show system status	Displays system status
21	show system dashboard	Displays the resources being used in the system currently
22	show system time	.
23	show system time setup	Displays Timezone and NTP configuration
24	show system traffic_meter	.
25	show system traffic_meter setup	Displays traffic meter configuration
26	show system usb-status	Displays USB Status
27	show system users	System group display mode
28	show system group	System user display mode
29	show system group specific*<row_id>*	Displays information for given group
30	show system group all	Displays all groups on system
31	show system users all	Displays all users on system
32	show system users specific*<row_id>*	Displays information for given user

33	show system group groupaccesscontrol *<group_id>*	Displays Group Access Control configuration for the selected group
34	show system group access_control_browser	Displays Access Control browsers Policies
35	show system group access_control_ip	Displays Access Control ips Policies
36	show system firmwareVersion	Displays the firmware Version.

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

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

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

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

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

1	show pop3-serverCheck	Displays status of Pop3 servers.

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

1	show Radius-serverCheck	Displays status of Radius servers.

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

1	show Radius-Settings	Displays RADIUS configuration. A RADIUS server maintains a database of user accounts used in larger environments. If a RADIUS server already exists, it can be used for authenticating users that want to connect to the wireless network provided by this device. When multiple RADIUS servers are configured, they are accessed in the same order as in the table. If first RADIUS server is not accessible, then system tries to contact to the next RADIUS server. **Configured Radius Servers** This table

		displays the list of all configured RADIUS servers. If the optional argument ServerIP is specified, detailed configuration of the RADIUS server is displayed. **Server IP:** IP address of RADIUS authentication server Accounting **Server IP:** IP address of RADIUS accounting server **Server Port:** RADIUS authentication server port to send the RADIUS messages. **Timeout:** The time (in seconds) the device waits for a response from the RADIUS server **Retries:** The number of tries the router will make to the RADIUS server before giving up. **Secret:** RADIUS server secret. This field is only displayed if the argument ServerIP is specified.

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

1	show net ipv6_tunnel status	Displays ipv6 tunnels status
2	show net bandwidth	.
3	show net bandwidth profile	.
4	show net bandwidth profile setup	Displays list of Available Bandwidth Profile(s).
5	show net bandwidth traffic_selector	.
6	show net bandwidth traffic_selector setup	Shows the list of Available Traffic Selector(s).
7	show net bandwidth profile interface_list	Displays the list of interface for Inbound Bandwidth Profile. It includes Available VLANs
8	show net bandwidth traffic_selector services	Displays a list of available services
9	show net ddns	.
10	show net ddns setup	Show Dynamic DNS Configuration.
11	show net lan dhcp	.
12	show net lan dhcp reserved_ip	.
13	show net lan dhcp reserved_ip setup	Shows a list of DHCP Reserved Addresses.
14	show net lan dhcp leased_clients	.
15	show net lan dhcp leased_clients list	Shows a list of Available DHCP Leased Clients.
16	show net dmz	.
17	show net dmz setup	Shows DMZ Configuration.
18	show net dmz dhcp	.

19	show net dmz dhcp reserved_ip	.
20	show net dmz dhcp reserved_ip setup	Displays a list of DMZ DHCP Reserved Addresses.
21	show net dmz dhcp leased_clients	.
22	show net dmz dhcp leased_clients list	Shows a list of Available DMZ DHCP Leased Clients.
23	show net ethernet	Displays Ethernet interfaces
24	show net lan	.
25	show net lan ipv4	.
26	show net lan ipv4 setup	Displays LAN Configuration.
27	show net lan ipv6	.
28	show net lan ipv6 setup	Shows IPv6 LAN Configuration.
29	show net statistics *<interface>*	Shows Interface Statistics
30	show net igmp	Displays igmp configuration
31	show net intel_Amt	Shows IntelAmt details
32	show net intel_Amt server	Shows IntelAmt Server Configuration
33	show net intel_Amt Reflector	show IntelAmt Reflector Configuration
34	show net intel_Amt server setup	Displays Intel_Amt server configuration.
35	show net intel_Amt Reflector setup	Displays Intel_Amt Reflector setup.
36	show net Ip_Alias	Shows Ip Alias configuration details.
37	show net Ip_Alias server	Shows Ip Alias configuration details.
38	show net Ip_Alias server setup	Displays net Intel_Amt server setup.
39	show net mode	.
40	show net mode setup	Displays IP MODE configuration
41	show net ipv6_tunnel	.
42	show net ipv6_tunnel setup	Displays ipv6 tunnels configuration
43	show net routing mode	.
44	show net routing mode setup	Routing Mode between WAN and LAN
45	show net wan wan1	.
46	show net wan wan1 ipv4	.
47	show net wan wan1 ipv4 status	Displays ipv4 wan1 Information.
48	show net wan wan1 ipv4 setup	Displays Wan1 Setup Information.
49	show net wan wan2	.
50	show net wan wan2 ipv4	.

51	show net wan wan2 ipv4 status	Displays ipv4 wan2 Information.
52	show net wan wan2 ipv4 setup	Displays wan2 Setup Information.
53	show net wan wan3	Displays the wan3 configuration
54	show net wan wan3 threeG	Shows ThreeG information.
55	show net wan wan3 threeG setup	Displays ThreeG Configuration.
56	show net wan wan3 threeG status	Displays wan3 ThreeG status.
57	show net wan	.
58	show net wan mode	Displays wan mode Setup.
59	show net wan port_setup	Displays wan port Setup.
60	show net wan vlan_setup	Displays vlan port Information for wan.
61	show net wan configurable_port	Displays configurable port Information.
62	show net wan wan1 ipv6	.
63	show net wan wan1 ipv6 status	Displays ipv6 wan1 Information.
64	show net wan wan1 ipv6 setup	Displays Wan1 Setup Information.
65	show net wan wan2 ipv6	.
66	show net wan wan2 ipv6 status	Displays ipv6 wan2 Information.
67	show net wan wan2 ipv6 setup	Displays Wan2 Setup Information.
68	show net routing ospfv2	Shows OSPFv2 Configuration
69	show net routing ospfv3	Shows OSPFv3 Configuration
70	show net routing ospfv2 setup	Displays OSPFv2 Configuration
71	show net routing ospfv3 setup	Displays OSPFv3 Configuration
72	show net routing protocol_binding	Shows protocol_binding rules
73	show net routing protocol_binding setup	Displays protocol Binding Rules
74	show net radvd	.
75	show net radvd setup	Displays RADVD configuration
76	show net routing dynamic	Shows dynamic routing setup
77	show net routing dynamic setup	Shows dynamic routing Setup.
78	show net routing	Displays routing setup
79	show net routing static	Displays Static Routes Info
80	show net routing static ipv4	Displays IPv4 Static Routes Info

81	show net routing static ipv4 setup	Shows all the configured IPV4 routes.
82	show net routing static interface_list	Shows all the interfaces on which static route can be configured
83	show net routing static ipv6	Displays IPv6 Static Routes Info
84	show net routing static ipv6 setup	Shows all the configured IPV6 Static routes.
85	show net upnp	Displays UPnP Information
86	show net upnp portmap	Displays UPnP portmap Table Information.
87	show net upnp setup	Displays UPnP Setup Information.
88	show net vlan	
89	show net vlan configuration	Displays VLAN Confgiuration.
90	show net multivlan	Shows vlan server status
91	show net multivlan subnet	Shows vlan server status
92	show net multivlan subnet status	Displays multi vlan Subnet List.
93	show net port-vlan	Shows Port vlan status
94	show net port-vlan status	Displays Port vlan status.
95	show net wireless_vlan	Shows Port vlan status
96	show net wireless_vlan status	Displays Port vlan status.

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

1	show ldap-serverCheck	Displays status of Ldap servers.

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

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

8	show security firewall custom_service setup	Displays a list of available Custom Service configuration
9	show security firewall	Displays Firewall Rules
10	show security firewall ipv4	Displays IPv4 Firewall Rules
11	show security firewall ipv4 setup	Displays IPv4 Firewall Rules
12	show security firewall algs	Displays ALGs protocals status
13	show security firewall ipv6	Displays IPv6 Firewall Rules
14	show security firewall ipv6 setup	Displays IPv6 Firewall Rules
15	show security ids	.
16	show security ids setup	Displays IDS configuration
17	show security session_settings	Displays Session Settings configuration
18	show security schedules	.
19	show security schedules setup	Displays Schedules configuration
20	show security firewall smtpAlg	.
21	show security firewall smtpAlg configure	.
22	show security firewall smtpAlg configure setup	Shows SmtpAlg Status.
23	show security firewall smtpAlg approvedMailId	.
24	show security firewall smtpAlg approvedMailId setup	Shows a List of Approved Mail_Id.
25	show security firewall smtpAlg blockedMailId	.
26	show security firewall smtpAlg blockedMailId setup	Shows a List of Blocked Mail_Id.
27	show security firewall smtpAlg subjectList	.
28	show security firewall smtpAlg subjectList setup	Shows a List of Subject, corresponding Mail_Id and Action.
29	show security mac_filter	.
30	show security mac_filter setup	Displays Source Mac Filter configuration
31	show security ip_or_mac_binding	.
32	show security ip_or_mac_binding setup	Displays IP/MAC Binding configuration

33	show security firewall vpn_passthrough	.
34	show security firewall vpn_passthrough setup	Displays VPN passthrough Configuration
35	show security webAccess	.
36	show security webAccess setup	Displays security webAccess configuration and rules Displays a list of Allowed IpAdrr/Network Web Access
37	show security website_filter	.
38	show security website_filter content_filtering	Displays content filtering configuration
39	show security website_filter approved_urls	Displays trusted domains configuration Displays a list of available Approved URLs
40	show security website_filter blocked_keywords	Displays blocked keywords configuration

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

1	vpn gre_tunnel	GRE Tunnel.
2	vpn gre_tunnel add	GRE Tunnel add mode
3	vpn gre_tunnel edit *<row_id>*	GRE Tunnel edit mode
4	vpn gre_tunnel delete *<row_id>*	GRE Tunnel delete mode
5	vpn l2tp client	Vpn policy mode.
6	vpn l2tp client configure	l2tp client configuration mode
7	vpn l2tp client_action *<action>*	Vpn l2tp client action set.
8	vpn l2tp	Vpn policy mode.
9	vpn l2tp server	Vpn policy mode.
10	vpn l2tp server configure	l2tp server configuration mode
11	vpn openvpn	Displays openvpn configure commands
12	vpn openvpn config	openvpn configuration mode
13	vpn openvpn remote_network	Opens vpn remote networks configuration commands.
14	vpn openvpn remote_network add	Adds a new remote network
15	vpn openvpn remote_network edit *<row_id>*	Remote network edit mode.
16	vpn openvpn remote_network delete *<row_id>*	Openvpn remote network delete mode.

17	vpn openvpn local_network	Opens vpn local networks configuration commands.
18	vpn openvpn local_network add	Adds a new local network.
19	vpn openvpn local_network edit *<row_id>*	Local network edit mode.
20	vpn openvpn local_network delete *<row_id>*	Openvpn local network delete mode.
21	vpn openvpn cert_upload	Openvpn local network display mode.
22	vpn openvpn cert_upload ca *<fileName> <ipAddr>*	Uploads the pem formatted CA Certificate.
23	vpn openvpn cert_upload server_client_cert *<fileName> <ipAddr>*	Uploads the pem formatted Server / Client Certificate.
24	vpn openvpn cert_upload client_key *<fileName> <ipAddr>*	Uploads the pem formatted Server/Client key.
25	vpn openvpn cert_upload dh_Key *<fileName> <ipAddr>*	Uploads the pem formatted Diffie Hellman key.
26	vpn openvpn cert_upload tls_Authkey *<fileName> <ipAddr>*	Uploads the pem formatted Tls Authentication Key.
27	vpn openvpn cert_upload crl_cert *<fileName> <ipAddr>*	Uploads the pem formatted CRL Certificate.
28	vpn openvpn cert_upload config *<fileName> <ipAddr>*	Uploads the pem formatted config file.
29	vpn pptp client	Vpn policy mode.
30	vpn pptp client configure	PPTP client configuration mode.
31	vpn pptp client_action *<action>*	Vpn pptp client action set.
32	vpn pptp	Vpn policy mode.
33	vpn pptp server	Vpn policy mode.
34	vpn pptp server configure	pptp server configuration mode
35	vpn sslvpn	sslvpn configuration commands
36	vpn sslvpn portal-layouts	sslvpn portal layout configuration commands
37	vpn sslvpn portal-layouts add	Adds sslvpn portal layout.
38	vpn sslvpn portal-layouts edit *<row_id>*	Edits sslvpn portal layout.
39	vpn sslvpn portal-layouts delete *<row_id>*	Deletes sslvpn portal layout.
40	vpn sslvpn portforwarding	Sslvpn portforwarding configuration commands.

41	vpn sslvpn portforwarding appconfig	Sslvpn portforwarding application configuration commands.
42	vpn sslvpn portforwarding appconfig add	Adds an application configuration rule.
43	vpn sslvpn portforwarding appconfig delete *<row_id>*	Deletes an application configuration rule.
44	vpn sslvpn portforwarding hostconfig	Sslvpn portforwarding host configuration commands.
45	vpn sslvpn portforwarding hostconfig add	Adds a host configuration rule.
46	vpn sslvpn portforwarding hostconfig delete *<row_id>*	Deletes a host configuration rule.
47	vpn sslvpn resource	Sslvpn resource configuration commands.
48	vpn sslvpn resource add	Adds an sslvpn resource.
49	vpn sslvpn resource configure	Configures an sslvpn resource.
50	vpn sslvpn resource configure add *<resource_name>*	Adds an sslvpn resource object.
51	vpn sslvpn resource configure delete *<row_id>*	Deletes an sslvpn resource object.
52	vpn sslvpn resource delete *<row_id>*	Deletes an sslvpn resource.
53	vpn sslvpn policy	Sslvpn policy configuration commands.
54	vpn sslvpn policy add	Adds an sslvpn policy.
55	vpn sslvpn policy edit *<row_id>*	Edits an sslvpn policy.
56	vpn sslvpn policy delete *<row_id>*	Deletes an sslvpn policy.
57	vpn sslvpn client	Sslvpn client configuration commands.
58	vpn sslvpn route	Sslvpn route configuration commands.
59	vpn sslvpn route add	Adds sslvpn client route.
60	vpn sslvpn route delete *<row_id>*	Deletes sslvpn client route.
61	vpn ipsec	Vpn policy mode.
62	vpn ipsec policy	Vpn policy mode.
63	vpn ipsec policy configure *<name>*	Vpn policy configuration mode.
64	vpn ipsec dhcp	Vpn ipsec over dhcp mode.
65	vpn ipsec dhcp configure	vpn dhcp over ipsec policy configuration mode
66	vpn ipsec policy enable *<name>*	Enables a vpn policy.
67	vpn ipsec policy disable *<name>*	Disables a vpn policy.

68	vpn ipsec policy delete *<name>*	Deletes a vpn policy.
69	vpn ipsec policy connect *<name>*	Connects a vpn tunnel.
70	vpn ipsec policy drop *<name>*	Drops a vpn tunnel.

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

1	dot11 profile	802.11 profile configuration commands.
2	dot11 accesspoint	802.11 access point configuration commands.
3	dot11 radio	802.11 radio configuration commands.
4	dot11 wds	802.11 wds configuration commands.
5	dot11 wmm	802.11 wmm configuration.
6	dot11 radius	802.11 radius configuration mode.
7	dot11 profile add *<profile_name>*	802.11 profile configuration mode.
8	dot11 profile edit *<profile_name>*	802.11 profile configuration mode.
9	dot11 wmm edit *<profile_name>*	802.11 wmm configuration mode.
10	dot11 radius configure	802.11 radius configuration mode.
11	dot11 profile delete *<profile_name>*	Deletes an 802.11 profile.
12	dot11 accesspoint add *<ap_name>*	802.11 access point configuration mode
13	dot11 accesspoint edit *<ap_name>*	802.11 access point configuration mode
14	dot11 accesspoint delete *<ap_name>*	Deletes an 802.11 access point.
15	dot11 wds enable *<radio_no>*	Enables wds.
16	dot11 wds disable *<radio_no>*	Disables wds.
17	dot11 wds add_peer *<radio_no> <mac_addr>*	Adds peer mac address wds.
18	dot11 wds delete_peer *<radio_no> <mac_addr>*	Deletes peer mac address wds.
19	dot11 accesspoint disable *<ap_name>*	Disables an 802.11 access point.
20	dot11 accesspoint enable *<ap_name>*	Enables an 802.11 access point.

21	dot11 radio configure *<radio_no>*	802.11 radio configuration mode.
22	dot11 radio advanced	Advanced radio configure
23	dot11 radio advanced configure *<radio_no>*	802.11 AP advanced configuration mode.
24	dot11 accesspoint wps	Advanced AP configure
25	dot11 accesspoint wps configure	802.11 AP wps configuration mode.
26	dot11 accesspoint acl	Accesspoint ACL configure commands
27	dot11 accesspoint ACL configure *<ap_name>*	802.11 AP ACL configuration mode.
28	dot11 accesspoint acl delete_mac_address *<rowid>*	Deletes acl mac address entry.

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

1	system POP3_Settings	System POP3 configuration commands.
2	system NT-Domain-Settings	Configures NT-Domain Settings
3	system Active-Directory-Settings	Configures Active-Directory Settings
4	system LDAP_Settings	Configures LDAP Settings
5	system POP3_Settings POP3_Server_Configuration	Configures POP3 Server
6	system POP3_Settings POP3_Trusted_CA	Uploads POP3 trusted Certificates
7	system logging	.
8	system logging ipv4	System logging ipv4 configuration.
9	system logging facility	System log Facility configuration.
10	system logging facility Options	System log Facility Options configuration.
11	system logging remote	System remote Logging configuration.
12	system logging ipv6	System ipv6 logs configuration.
13	system logging ipv4 configure	System logging configuration mode.
14	system logging facility configure *<facility>*	System logging facility configuration mode.
15	system logging remote configure	System remote Logging configuration mode.
16	system logging ipv6 configure	System ipv6 logs configuration mode.
17	system Radius-Settings	Configures Radius-Settings.
18	system remote_management	Remote Mgmt Setup.

19	system remote_management https	Remote Mgmt Setup for https.
20	system remote_management https configure	Configures remote management support for https.
21	system remote_management telnet configure	Configures remote management support for telnet.
22	system sessionSettings	Session Settings Configuration.
23	system sessionSettings admin	Session Settings Configuration.
24	system sessionSettings admin configure	Admin Session Settings Configuration.
25	system sessionSettings guest	Session Settings Configuration.
26	system sessionSettings guest configure	Guest Session Settings Configuration.
27	system snmp	System SNMP configuration
28	system snmp trap	System SNMP trap configuration.
29	system snmp sys	System SNMP system configuration.
30	system snmp access	System SNMP Access Configuration.
31	system snmp users	System SNMP v3 User Configuration.
32	system snmp trap configure *<agent_ip>*	SNMP trap configuration mode.
33	system snmp trap delete *<agent_ip>*	Deletes a SNMP trap configuration.
34	system snmp users configure *<user>*	SNMP v3 User list configuration settings
35	system snmp sys configure	SNMP system configuration mode
36	system snmp access add	SNMP access configuration mode
37	system snmp access edit *<rowid>*	SNMP configuration mode
38	system snmp access delete *<rowid>*	SNMP access configuration mode
39	system switch_settings	Switch setting setup.
40	system switch_settings power_saving	Power saving setup.
41	system switch_settings jumbo_frame	Jumbo frame setup.
42	system switch_settings power_saving configure	Power saving configuration mode.
43	system switch_settings jumbo_frame configure	Jumbo frame configuration mode.
44	system admin_setting	System configuration.

45	system admin_setting configure	System configuration mode.
46	system time	System time configuration mode
47	system time configure	System time configuration mode
48	system traffic_meter	Traffic meter Configuration setup.
49	system traffic_meter configure	Traffic meter configuration mode.
50	system usb	USB Configuration.
51	system usb usb1	USB1 Configuration.
52	system usb usb1 configure	USB1 Configuration.
53	system usb safelyRemoveUsb	Safely removing the USB.
54	system usb SafelyRemoveUSB usb1	To unmount usb1
55	system usb SafelyRemoveUSB usb2	To unmount usb2
56	system usb usb2	USB2 Configuration.
57	system usb usb2 configure	USB2 Configuration.
58	system usb shareport_vlan	USB SharePort settings.
59	system usb shareport_vlan configure *<row_id>*	SharePort on vlan configuration.
60	system usb shareport_vlan show	Displays SharePort on vlan configuration.
61	system users	System user configuration commands.
62	system group	System group configuration commands.
63	system group add	System groups add mode.
64	system group edit *<row_id>*	System groups edit mode.
65	system group delete *<row_id>*	System groups delete mode.
66	system users add	System users add mode.
67	system users edit *<row_id>*	System users edit mode.
68	system users delete *<row_id>*	System users delete mode.
69	system group groupaccesscontrol	Group access control.
70	system group groupaccesscontrol configure *<group_id>*	Group access control configuration.
71	system group access_control_browser	List of browsers for which login policies can be applied.
72	system group access_control_browser add	Adds a browser to Access Control browsers list

73	system group access_control_browser delete *<row_id>*	Deletes a browser from Access Control browsers list.
74	system group access_control_ip	List of ip for which login policies can be applied
75	system group access_control_ip add	Adds an ip to Access Control ip list.
76	system group access_control_ip delete *<row_id>*	Deletes an ip from Access Control ip list.

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

1	util restore-factory-defaults	Revert to factory default settings.
2	util system_check	System check options
3	util system_check ping *<ip_address>*	Pings an Internet Address.
4	util system_check dns_lookup *<dns>*	To retrieve the IP address of a Web, FTP, Mail or any other Server on the Internet
5	util system_check traceroute *<ip_address>*	Displays all the routers present between the destination IP address and this router
6	util system_check display_IPV4_routingtable	Displays IPV4 Routing Table
7	util system_check display_IPV6_routingtable	Displays IPV6 Routing Table
8	util system_check capturePackets	Allows you to capture all packets that pass through the selected interface
9	util system_check capturePackets start *<interface>*	Starts the packet capture
10	util system_check capturePackets avail_interfaces	Displays available interfaces for packet capture
11	util system_check capturePackets stop	Stops the packet capture
12	util system_check capturePackets download *<fileName><ipAddr>*	Downloads the packet capture to the host machine
13	util dbglog_download *<fileName> <ipAddr>*	Downloads Dbglogs to the host machine
14	util reboot	Reboots the system.

15	util usb_test *<ipAddr> <fileNam e>*	To test the USB.
16	util firmware_upgrade *<IpAddr> <FileName>*	To upgrade the firmware.
17	util enable_auto_backup *<statu s>*	Enables/Disables Auto Backup support.
18	util enable_config_encryp *<stat us>*	Enables/Disables Configuration encryption support.
19	util watchdog_disable *<status>*	Disables/Enables watchdog timer.

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

1	license list	List license on the device.
2	license activate *<activationKey>*	Activates a license on the device.

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

1	net ipv6_tunnel	Ipv6 tunnel configuration setup.
2	net ipv6_tunnel six_to_four	Six to four tunnel configuration setup.
3	net ipv6_tunnel six_to_four configure	Six To Four Tunnel configuration mode.
4	net bandwidth	.
5	net bandwidth profile	It gives options to add/edit/delete a bandwidth profile.
6	net bandwidth profile enable *<enable>*	It allows to enable/disable bandwidth profiles.
7	net bandwidth profile add	It allows to add a bandwidth profile.
8	net bandwidth profile edit *<row_id>*	It allows to edit a bandwidth profile.
9	net bandwidth profile delete *<row_id>*	It allows to delete a bandwidth profile.
10	net bandwidth traffic_selector	It gives options to add/edit/delete a traffic selector for a bandwidth profile.
11	net bandwidth traffic_selector add	It allows to add a traffic selector for a bandwidth profile.
12	net bandwidth traffic_selector edit *<row_id>*	It allows to edit a traffic selector for a bandwidth profile.

13	net bandwidth traffic_selector delete *<row_id>*	It allows to delete a traffic selector for a bandwidth profile.
14	net ddns	DDNS setup.
15	net ddns wan1	DDNS setup.
16	net ddns wan2	DDNS setup.
17	net ddns wan1 configure	DDNS configuration mode.
18	net ddns wan2 configure	DDNS configuration mode.
19	net lan dhcp	DHCP setup.
20	net lan dhcp reserved_ip	DHCP Reserved IPs setup.
21	net lan dhcp reserved_ip configure *<mac_address>*	DHCP Reserved IPs add/edit mode.
22	net lan dhcp reserved_ip delete *<mac_address>*	Deletes a specific reserved ip entry.
23	net dmz dhcp	DHCP setup.
24	net dmz dhcp reserved_ip	DHCP Reserved IPs setup.
25	net dmz dhcp reserved_ip configure *<mac_address>*	DHCP Reserved IPs add/edit mode.
26	net dmz dhcp reserved_ip delete *<mac_address>*	Deletes a specific reserved ip entry.
27	net ethernet	Ethernet configuration.
28	net ethernet configure *<interface_name>*	Ethernet configuration mode.
29	net lan	LAN setup.
30	net lan ipv4	.
31	net lan ipv4 configure	IPv4 LAN configuration mode.
32	net lan ipv6	.
33	net lan ipv6 configure	IPv6 LAN configuration mode.
34	net lan ipv6 pool	.
35	net lan ipv6 pool configure *<ipv6PoolStartAddr>*	IPv6 LAN configuration add/edit mode.
36	net lan ipv6 pool delete *<ipv6PoolStartAddr>*	IPv6 LAN configuration delete mode.
37	net igmp	Igmp configuration commands.
38	net igmp configure	Specifies igmp proxy should be enable or disable
39	net intel_Amt	Net policy mode.
40	net intel_Amt server	Net policy mode.
41	net intel_Amt server configure	Intel Amt server configuration mode
42	net intel_Amt_Reflector	Net policy mode.
43	net intel_Amt_Reflector configure	Intel Amt Reflector configuration mode

44	net ip_Aliasing	Net policy mode.
45	net ip_Aliasing server	Net policy mode.
46	net ip_Aliasing server add	Adding Ip Aliasing server configuration
47	net ip_Aliasing server edit *<row_id>*	Editing Ip Aliasing server configuration.
48	net ip_Aliasing server delete *<row_id>*	Deleting Ip Aliasing configuration
49	net mode	IP Mode Setup
50	net mode configure	IP Mode configuration mode.
51	net ipv6_tunnel isatap	Isatap tunnel configuration commands.
52	net ipv6_tunnel isatap add	Isatap tunnel configuration add mode.
53	net ipv6_tunnel isatap edit *<row_id>*	Isatap Tunnel configuration edit mode.
54	net ipv6_tunnel isatap delete *<row_id>*	Isatap tunnel configuration delete mode.
55	net routing mode	Routing Mode between WAN and LAN setup.
56	net routing mode configure	Routing Mode between WAN and LAN configuration mode.
57	net wan wan1	Wan configuration mode.
58	net wan wan1 ipv4	Ipv4 wan configuration mode.
59	net wan wan1 ipv4 configure	Ipv4 wan wan1 configuration mode..
60	net wan wan2	Wan configuration mode.
61	net wan wan2 ipv4	Ipv4 wan configuration mode.
62	net wan wan2 ipv4 configure	Ipv4 wan wan2 configuration mode.
63	net wan wan3	Wan3 configuration mode.
64	net wan wan3 threeG	Wan3 configuration mode.
65	net wan wan3 threeG configure	ThreeG wan wan3 configuration mode.
66	net wan	Net wan configuration mode.
67	net wan mode	Net wan configuration mode.
68	net wan mode configure	Net wan configuration mode.
69	net wan port_setup	Displays net wan port configuration.
70	net wan port_setup configure	Displays wan port configuration mode.
71	net wan vlan_setup	Displays wan vlan setup.
72	net wan vlan_setup configure	Displays wan vlan configuration mode.
73	net wan vlan_setup vlanId_Add	Displays wan vlan Id Add mode.
74	net wan vlan_setup vlanId_Delete	Displays wan vlan Id delete mode.
75	net wan configurable_port	Net wan configurable port setup.
76	net wan configurable_port configure	Net wan configurable port setup.

77	net wan wan1 ipv6	Displays ipv6 wan configuration mode
78	net wan wan1 ipv6 configure	Displays ipv6 wan1 configuration mode
79	net wan wan2 ipv6	Displays ipv6 wan2 configuration mode
80	net wan wan2 ipv6 configure	Displays ipv6 wan2 configuration mode
81	net routing ospfv2	Displays OSPF Configuration for IPV4
82	net routing ospfv3	Displays OSPF Configuration for IPV6
83	net routing ospfv2 configure *<interface>*	Displays ospfv2 configuration mode.
84	net routing ospfv3 configure *<interface>*	Displays ospfv3 configuration mode.
85	net routing protocol_binding	Displays protocol_binding configuration commands
86	net routing protocol_binding add	Protocol_binding rules configuration add mode.
87	net routing protocol_binding edit *<row_id>*	To edit the selected protocol_binding
88	net routing protocol_binding enable *<row_id>*	Protocol_binding rules configuration mode.
89	net routing protocol_binding disable *<row_id>*	Protocol_binding rules configuration mode.
90	net routing protocol_binding delete *<row_id>*	Protocol_binding rules configuration mode.
91	net radvd	RADVD configuration setup.
92	net radvd pool	RADVD configuration setup.
93	net radvd configure	RADVD configuration mode.
94	net radvd pool add	RADVD Pool configuration mode.
95	net radvd pool edit *<row_id>*	RADVD Pool configuration mode.
96	net radvd pool delete *<row_id>*	RADVD pool configuration mode.
97	net routing dynamic	Configures the routes dynamically.
98	net routing dynamic configure	Configures the routes dynamically.
99	net routing	Configures routing mode, static and dynamic route(s).
100	net routing static	Configures the routes.
101	net routing static ipv4	Configures the IPv4 routes.
102	net routing static ipv6	Configures the IPV6 routes.
103	net routing static ipv4 configure *<name>*	Adds new IPv4 static routes.
104	net routing static ipv6 configure *<name>*	Adds new IPV6 static routes.
105	net routing static ipv4 delete *<name>*	Deletes a specific IPv4 route.
106	net routing static ipv6 delete *<name>*	Deletes a specific IPV6 route.

107	net routing static ipv4 deleteAll	Deletes all the configured IPv4 routes.
108	net routing static ipv6 deleteAll	Deletes all the configured IPv6 routes.
109	net tahi	Settings for tahi test suite.
110	net tahi add-default-route *<ip_address>*	Adds ipv6 default route on lan interface.
111	net tahi delete-default-route	Deletes ipv6 default route on lan interface.
112	net tahi add-route *<ip_address> <gw>*	Adds ipv6 route on lan interface.
113	net tahi del-route *<ip_address> <gw>*	Adds ipv6 route on lan interface.
114	net tahi stop-RA	Stop sending RA.
115	net tahi start-RA-AdvRetransTimer(1000)	Starts sending RA with AdvRetransTimer as 1000.
116	net tahi start-RA-AdvRetransTimer(5000)	Starts sending RA with AdvRetransTimer as 5000.
117	net tahi startRA-Reachable(30000)Retrans(1000)	Starts sending RA with AdvReachableTime as 30000 and AdvRetransTimer as 1000.
118	net tahi start-RA-AdvReachableTime(10000)	Starts sending RA with AdvReachableTime as 10000.
119	net tahi start-RA-AdvReachableTime(30000)	Starts sending RA with AdvReachableTime as 30000.
120	net tahi start-RA(Default)	Starts sending RA with default parameters.
121	net tahi start-RA-MinValues	Starts sending RA with minimum values of parameters.
122	net tahi start-RA-MaxValues	Starts sending RA with maximum values of parameters.
123	net tahi start-RA-MaxRtrAdvInterval(10)	Starts sending RA with MaxRtrAdvInterval value of 10.
124	net tahi start-RA-MaxRtrAdvInterval(40)	Starts sending RA with MaxRtrAdvInterval value of 40.
125	net tahi start-RA-MinRtrAdvInterval(198)	Starts sending RA with MinRtrAdvInterval value of 198.
126	net tahi start-RA-prefix(8000::)	Starts sending RA with prefix 8000::/64.
127	net tahi start-RA-prefix(fec0::)	Starts sending RA with prefix fec0::/64.
128	net tahi start-RA-AdvCurHopLimit(0)	Starts sending RA with AdvCurHopLimit value as 0.
129	net tahi start-RA-AdvCurHopLimit(15)	Starts sending RA with AdvCurHopLimit value as 15.
130	net tahi start-RA-WAN	Starts sending RA on the WAN interface.
131	net tahi ipv6-down	Disables the ipv6 stack on the router.

132	net tahi ipv6-up	Enables the ipv6 stack on the router.
133	net tahi ipv6-global-up	Enables the ipv6 stack on the router, and adds global ip.
134	net tahi ipv6-Alias-Add(LAN) *<ip6_address>*	Adds ipv6 address to LAN interface.
135	net tahi ipv6-Alias-Del(LAN) *<ip6_address>*	Deletes an ipv6 address from LAN interface.
136	net tahi ipv6-Alias-Add(WAN) *<ip6_address>*	Adds ipv6 address to WAN interface.
137	net tahi ipv6-Alias-Del(WAN) *<ip6_address>*	Deletes an ipv6 address from WAN interface.
138	net tahi neigh-cache-del	Deletes the ipv6 neighbor cache.
139	net tahi reachable-time *<time>*	Sets the reachable time of neighbour cache entries
140	net tahi mcast-start	Starts ipv6 multicast.
141	net tahi mcast-stop	Stops ipv6 multicast.
142	net tahi ping6 *<ip> <size>*	Ping6 on LAN interface with count one.
143	net tahi mping6 *<mip>*	Multicast ping6 on LAN.
144	net tahi bping6 *<bip> <psize>*	ping6
145	net tahi pmtu-route-add *<ipAdd>*	Adds ipv6 route on lan interface.
146	net tahi disable-ipv6-firewall	Disables ipv6 firewall.
147	net tahi show-LAN-ip	Shows ipv6 addresses of LAN interface.
148	net tahi interface-down *<interface>*	Brings selected interface down.
149	net tahi interface-up *<interface>*	Brings selected interface up.
150	net tahi start-RA-custom *<fileName> <ipAddr>*	Starts RA with configuration file obtained through tftp.
151	net tahi RA-Start	Starts RA with custom configuration.
152	net ipv6_tunnel teredo	Teredo tunnel configuration setup.
153	net ipv6_tunnel teredo configure	Teredo Tunnel configuration mode.
154	net upnp	Upnp configuration mode
155	net upnp configure	Upnp configuration mode
156	net port-vlan	port vlan
157	net port-vlan lan_edit *<portnamew>*	Vlan port name range 1-4.
158	net port-vlan wlan_edit *<ssidName>*	SSID to be edited. Use command 'show net wireless_vlan status 'to dislay all SSID's Name
159	net vlan-membership	Vlan-membership
160	net vlan-membership lan_edit *<portw>*	Net vlan membership for the vlan and Wlan port.

161	net vlan-membership wlan_edit *<ssidName>*	SSID to be edited. Use command 'show net wireless_vlan status 'to dislay all SSID's Name
162	net multivlan	Multivlan server configure
163	net multivlan subnet	Multivlan Server configure
164	net multiVlan subnet edit *<vlanID>*	Multivlan server edit mode
165	net vlan	Displays vlan Configuration Settings.
166	net vlan config	Displays vlan configuration.
167	net vlan config add *<vlan_id>*	Adds a vlan.
168	net vlan config edit *<vlan_Id>*	Edits a configured vlan.
169	net vlan config delete *<VlanId>*	Deletes a vlan.
170	net vlan config enable	Enables vlan configuration.
171	net vlan config disable	Disables vlan configuration.
172	net dmz	Dmz configuration mode.
173	net dmz configure	Dmz configuration mode.

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

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

13	security firewall custom_service delete *<row_id>*	Custom services configuration delete mode.
14	security firewall	Firewall rules setup.
15	security firewall ipv4	Firewall IPv4 rules setup.
16	security firewall ipv4 configure	Firewall IPV4 rules configuration mode.
17	security firewall ipv4 default_outbound_policy *<default_outbound_policy>*	Firewall Settings, Default Outbound Policy configuration mode.
18	security firewall ipv4 edit *<row_id>*	To edit the selected Firewall IPV4.
19	security firewall ipv4 enable *<row_id>*	To Enable Firewall IPV4 rules configuration mode.
20	security firewall ipv4 disable *<row_id>*	To Disable Firewall IPV4 Rules configuration mode.
21	security firewall ipv4 delete *<row_id>*	To delete the selected Firewall IPV4 Rule.
22	security firewall ipv4 move *<row_id>*	Firewall IPV4 Rule reordering mode.
23	security firewall algs	Firewall ALGs configuration mode.
24	security firewall ipv6	Firewall IPv6 rules setup.
25	security firewall ipv6 configure	Firewall IPV6 rules configuration mode.
26	security firewall ipv6 edit *<row_id>*	To edit the selected Firewall IPV6 rule.
27	security firewall ipv6 enable *<row_id>*	To enable Firewall IPV6 rules configuration mode.
28	security firewall ipv6 disable *<row_id>*	To disable Firewall IPV6 Rules configuration mode.
29	security firewall ipv6 delete *<row_id>*	To delete the selected Firewall IPV6 Rule
30	security firewall ipv6 move *<row_id>*	Firewall IPV6 Rule reordering mode.
31	security firewall ipv6 default_outbound_policy *<default_outbound_policy>*	Firewall Settings, IPv6 Default Outbound Policy configuration mode.
32	security ids	IDS Configuration setup.
33	security ids configure	IDS configuration mode.
34	security session_settings	Session Settings Configuration setup.
35	security session_settings configure	Session Settings configuration mode.
36	security schedules	Schedules Configuration setup.
37	security schedules add	To add new Schedule.

38	security schedules edit *<row_id>*	To edit the selected Schedule.
39	security schedules delete *<row_id>*	To delete the selected schedule.
40	security firewall smtpAlg	SmtpAlg configuration setup.
41	security firewall smtpAlg approvedMailId	To list the MailId approved by the user.
42	security firewall smtpAlg blockedMailId	Lists the blockedMailIds.
43	security firewall smtpAlg subjectList	To list all the subjects and Mail ids.
44	security firewall smtpAlg configure	SmtpAlg configuration mode.
45	security firewall smtpAlg approvedMailId add	It allows Configuration of the approved MailId.
46	security firewall smtpAlg approvedMailId edit *<row_id>*	It allows to edit an approved MailId.
47	security firewall smtpAlg approvedMailId delete *<row_id>*	It allows to delete an approved MailId.
48	security firewall smtpAlg blockedMailId add	It allows to Configure a blocked MailId.
49	security firewall smtpAlg blockedMailId edit *<row_id>*	It allows to edit a blocked MailId.
50	security firewall smtpAlg blockedMailId delete *<row_id>*	It allows to delete a blocked MailId.
51	security firewall smtpAlg subjectList add	It allows to add subject with MailId and action.
52	security firewall smtpAlg subjectList edit *<row_id>*	It allows to edit subject with MailId and action.
53	security firewall smtpAlg subjectList delete *<row_id>*	It allows to delete the configuration.
54	security mac_filter	Source mac filter configuration mode.
55	security ip_or_mac_binding	Ip mac binding configuration mode.
56	security mac_filter configure	Source mac filter configuration mode.
57	security mac_filter source	.
58	security mac_filter source add	To add a new mac address.
59	security mac_filter source edit *<row_id>*	To edit the selected mac address from the list.
60	security mac_filter source delete *<row_id>*	To delete the selected mac address.
61	security ip_or_mac_binding add	To link to the ip/mac binding configuration mode.

62	security ip_or_mac_binding edit *<row_id>*	To edit the selected rule in the ip/mac binding configuration page.
63	security ip_or_mac_binding delete *<row_id>*	To delete the selected rule/rules.
64	security firewall vpn_passthrough	VPN Passthrough setup.
65	security firewall vpn_passthrough configure	VPN Passthrough configuration mode.
66	security webAccess	Web Access Filter Configuration setup.
67	security webAccess status *<status>*	Displays security webAccess status
68	security webAccess add	Security webAccess add.
69	security webAccess edit *<row_id>*	Security webAccess edit.
70	security webAccess delete *<row_id>*	Security webAccess delete.
71	security website_filter	Website filtering configuration setup.
72	security website_filter content_filtering	Content filtering configuration setup.
73	security website_filter approved_urls	Trusted domains configuration setup.
74	security website_filter blocked_keywords	Blocked keywords configuration setup.
75	security website_filter content_filtering configure	Content filtering configuration mode.
76	security website_filter approved_urls add	To add the approved URL configuration page
77	security website_filter approved_urls edit *<row_id>*	To edit the selected URL configuration.
78	security website_filter approved_urls delete *<row_id>*	To delete the selected URL configuration.
79	security website_filter blocked_keywords add	Blocked Keyword configuration mode.
80	security website_filter blocked_keywords edit *<row_id>*	To edit the selected Blocked Keywords configuration mode.
81	security website_filter blocked_keywords delete *<row_id>*	To delete the selected blocked Keywords configuration mode.
82	security website_filter blocked_keywords enable *<row_id>*	To enable the blocked Keywords configuration mode.
83	security website_filter blocked_keywords disable *<row_id>*	To disable the blocked Keywords configuration mode.

Chapter 6. Configuration commands under branch VPN

6.1 vpn gre_tunnel add

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

6.2 vpn gre_tunnel edit *<row_id>*

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

6.3 vpn gre_tunnel delete *<row_id>*

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

6.4 vpn l2tp client configure

S.No	Command Name	Description	Type and Description
1	save	Saves l2tp client configuration settings.	
2	cancel	To revert to the previous settings.	
3	exit	Saves l2tp client configuration settings, and exit current mode.	
4	enable	Enables/disables L2TP client.	Boolean choice
5	server_address	L2TP server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	remote_network	Network Address of remote network which is local to L2TP Server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	remote_subnet	Remote Network Subnet Mask.	number in range of 1 to 32
8	username	Username allocated to L2TP client to connect to L2TP server.	String
9	password	Password allocated to client.	String
10	mppe_enable	Enables mppe encryption.	Boolean choice
11	reconnect_mode	Selects reconnect mode.	Reconnect Mode type
12	time_out	If there is no traffic from a user for more than the specified time out, the connection is disconnected.	Radius client authentication timeout Type.

6.5 vpn l2tp client_action *<action>*

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

6.6 vpn l2tp server configure

S.No	Command Name	Description	Type and Description
1	save	Saves l2tp server configuration settings.	

S.No	Command Name	Description	Type and Description
2	cancel	To revert to the previous settings.	
3	exit	Saves l2tp server configuration settings, and exits current mode.	
4	enable_v4	Enables/disables L2TP server in IPv4 mode only.	Boolean choice
5	enable_v6	Enables/disables L2TP server in IPv4/IPv6 mode.	Boolean choice
6	Routing_mode	Select L2TP routing mode.	Select Route Mode
7	start_address	L2TP server starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	end_address	L2TP server ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	ipv6_prefix	L2TP server IPv6 Prefix.	String
10	ipv6_prefix_length	L2TP server IPv6 Prefix length.	Unsigned integer
11	Authentication_type	Selects the type of Authentication required.	Authentication type
12	EnablePap	Enables PAP authentication.	Boolean choice
13	EnableChap	Enables CHAP authentication.	Boolean choice
14	EnableMSChap	Enables MS-CHAP authentication.	Boolean choice
15	EnableMSChapv2	Enables MS-CHAPv2 authentication.	Boolean choice
16	l2tpSecretKeyEnable	Enables/Disables support for Secret Key, and enters Secret Key if support is enabled.	Boolean choice
17	secretKey	Enter L2TP secret Key if Secret Key is enabled.	String
18	timeout	If there is no traffic from a user for more than the specified time out, the connection is disconnected.	Radius client authentication timeout Type.

6.7 vpn openvpn config

S.No	Command Name	Description	Type and Description
1	save	Saves openvpn configuration settings.	
2	cancel	To revert to previous settings openvpn configuration settings	
3	exit	Saves openvpn configuration settings, and exit current mode.	
4	enable	Enables/disables openvpn client/server.	Boolean choice
5	mode	OpenVPN daemon mode. It can run in server mode, client mode or access server client mode	OpenVPN daemon mode.
6	server_identifier_type	OpenVPN server identifier type.	OpenVPN server identifier type
7	server_ip	OpenVPN server IP address/FQDN to which the client connect.	
8	server_ip ip_address	OpenVPN server IP address to which the client connect.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
9	server_ip fqdn	OpenVPN server FQDN to which the client connect.	String
10	vpn_network	Address of the Virtual Network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	vpn_netmask	Netmask of the Virtual Network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	port	The port number on which openvpn server (or Access Server) runs.	Port number
13	tunnel_protocol	The protocol used to communicate with the remote host. E.g.TCP, UDP. UDP is the default.	The protocol used to communicate with the remote host
14	encription_algorithm	The cipher with which the packets are encrypted. E.g. BF-CBC, AES-128, AES-192 and AES-256. BF-CBC is the default	The cipher with which the packets are encrypted
15	hash_algorithm	Message digest algorithm used to	Message digest algorithm used to authenticate packets.

S.No	Command Name	Description	Type and Description
		authenticate.packets. E.g.: SHA1, SHA256 and SHA512. SHA1 is the default.	
16	tunnel_type	Selects Full Tunnel to redirect all the traffic through the tunnel. Select Split Tunnel to redirect traffic to only specified resources (added from openVpnClient Routes) through the tunnel. Full Tunnel is the default.	type of tunnel
17	allow_client_to_client	Enables this to allow openvpn clients to communicate with each other in split tunnel case. Disabled by default.	Boolean choice
18	select_primaryCert	Enables this to select the Set of certificates and keys the server uses. Enable this for first time configuration.	Boolean choice
19	select_secondaryCert	Enables this to select Set of certificates and keys newly uploaded.	Boolean choice
20	enable_tls_authkey	Enabling this adds Tls authentication which adds an additional layer of authentication. Can be checked only when the tls key is uploaded. Disabled by default.	Boolean choice
21	block_invalid_client_certificates	Enabling this blocks invalid client certificates based on the CRL certificate uploaded. Can be checked only when the CRL certificate is uploaded. Disabled by default.	Boolean choice

6.8 vpn openvpn remote_network add

S.No	Command Name	Description	Type and Description
1	save	Saves Remote network Configuration settings.	
2	cancel	To revert to previous settings.	
3	exit	Saves Remote network configuration settings, and exits current mode.	
4	common_name	Common Name of the OpenVPN client certificate	String
5	remote_network	Network address of the remote resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	remote_netmask	Netmask of the remote resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

6.9 vpn openvpn remote_network edit *<row_id>*

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

6.10 vpn openvpn remote_network delete *<row_id>*

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

6.11 vpn openvpn local_network add

S.No	Command Name	Description	Type and Description
1	save	Save local network settings.	
2	cancel	To revert to previous local network settings.	
3	exit	Save local network configuration settings and exit current mode.	
4	local_network	Network address of the local resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	local_netmask	Netmask of the local resource.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

6.12 vpn openvpn local_network edit *<row_id>*

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

6.13 vpn openvpn local_network delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes the selected openvpn Local network.	Unsigned integer

6.14 vpn openvpn cert_upload ca *<fileName> <ipAddr>*

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

6.15 vpn openvpn cert_upload server_client_cert *<fileName> <ipAddr>*

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

6.16 vpn openvpn cert_upload client_key *<fileName> <ipAddr>*

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

6.17 vpn openvpn cert_upload dh_Key *<fileName> <ipAddr>*

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

6.18 vpn openvpn cert_upload tls_Authkey *<fileName> <ipAddr>*

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

6.19 vpn openvpn cert_upload crl_cert *<fileName> <ipAddr>*

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

6.20 vpn openvpn cert_upload config *<fileName> <ipAddr>*

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

6.21 vpn pptp client configure

S.No	Command Name	Description	Type and Description
1	save	Saves pptp client configuration settings.	
2	cancel	To revert to previous PPTP Client configuration settings.	
3	exit	Saves pptp client configuration settings, and exits current mode.	
4	enable	Enables/disables PPTP client.	Boolean choice
5	server_address	PPTP server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	remote_network	Network Address of remote network which is local to PPTP Server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	remote_subnet	Remote Network Subnet Mask.	Number in range of 1 to 32.
8	username	Username allocated to client to connect to PPTP Server.	String
9	password	Password allocated to client to connect to PPTP Server.	String
10	mppe_enable	Enables mppe encryption.	Boolean choice
11	time_out	Specified time after which the connection is disconnected.	Unsigned integer

6.22 vpn pptp client_action *<action>*

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

6.23 vpn pptp server configure

S.No	Command Name	Description	Type and Description
1	save	Saves pptp server configuration settings.	
2	cancel	To revert to the previous pptp server configuration settings.	

S.No	Command Name	Description	Type and Description
3	exit	Saves pptp server configuration settings, and exits current mode.	
4	enable_v4	Enables/disables PPTP server in IPv4 mode only.	Boolean choice
5	enable_v6	Enables/disables PPTP server in IPv4/IPv6 mode.	Boolean choice
6	Routing_Mode	Selects Routing mode.	Select Route Mode
7	start_address	PPTP server starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	end_address	PPTP server ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	ipv6_prefix	PPTP server IPv6 Prefix.	String
10	ipv6_prefix_length	PPTP server IPv6 Prefix length.	Unsigned integer
11	Authentication_type	Selects the type of authentication required.	Authentication type
12	pap_enable	Enables support for PAP authentication method.	Boolean choice
13	chap_enable	Enables support for CHAP authentication method.	Boolean choice
14	mschap_enable	Enables support for MS-CHAP authentication method.	Boolean choice
15	mschapv2_enable	Enables support for MS-CHAPv2 authentication method.	Boolean choice
16	Mppe40Enable	Enables Mppe 40 bit encryption	Boolean choice
17	Mppe128Enable	Enables Mppe 128 bit encryption	Boolean choice
18	MppeStatefulEnable	Enables Stateful Mppe encryption	Boolean choice
19	UserTimeOut	The specified time after which the connection is disconnected.	Radius client authentication timeout Type.
20	Enable_Netbios	Enables/Disables the Netbios functionality.	Boolean choice
21	Primary_Wins_Server	Enter primary Windows server ip Address here.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
22	Secondary_Wins_Server	Enter Secondary Windows server ip address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

6.24 vpn sslvpn portal-layouts add

S.No	Command Name	Description	Type and Description
1	save	Saves portal settings.	
2	exit	Saves portal settings, and exits current mode.	
3	cancel	To revert to previous portal settings.	
4	portal_name	Specifies the portal name	String, Max 32 characters and no ' or empty space or "
5	profile_name	Specifies the profile name	String, Max of 32 alpha numeric characters
6	portal_title	Specifies the web browser window title for the portal.	String, Max 64 characters and no ' or empty space or "
7	banner_title	Specifies the banner title to Displays to users before logging into the portal.	String, MAX 64 characters, ' is not supported;
8	banner_message	Specifies the banner message that would be displaysed along with the banner title.	String, 'character is not supported;
9	display_banner	Specifies whether the banner message and banner title should be displayed.	Boolean choice
10	enable_httpmetatags	Specifies whether the http meta tags should be enabled.	Boolean choice
11	enable_activexwebcachecleaner	Specifies whether the activex web cache cleaner should be enabled.	Boolean choice
12	enable_vpntunnel	Specifies whether the vpn tunnel should be enabled	Boolean choice
13	enable_portforwarding	Specifies whether the port forwarding should be enabled.	Boolean choice
14	sslAuthType	Selects the authentication type for the portal.	Supported authentication type
15	SSL_GROUP	Selects a group name for the portal (only for local authentication).	String, Max 32 characters and no ' or empty space or "

6.25 vpn sslvpn portal-layouts edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Edits sslvpn portal layout	Unsigned integer
2	save	Saves portal settings	
3	exit	Saves portal settings and exit current mode	
4	cancel	To revert to previous settingsTo revert to the previous settings	
5	profile_name	Specifies the profile name	String, Max 32 characters and no ' or empty space or "
6	portal_title	Specifies the portal title	String, Max 64 characters and no ' or empty space or "
7	banner_title	Specifies the banner title to Displays to users before logging into the portal.	String, MAX 64 characters, ' is not supported;
8	banner_message	Specifies the banner message that would be displayed along with the banner title.	String, ' character is not supported;
9	display_banner	Specifies whether the banner message and banner title should be displayed.	Boolean choice
10	enable_httpmetatags	Specifies whether the http meta tags should be enabled.	Boolean choice
11	enable_activexwebcachecleaner	Specifies whether the activex web cache cleaner should be enabled.	Boolean choice
12	enable_vpntunnel	Specifies whether the vpn tunnel should be enabled	Boolean choice
13	enable_portforwarding	Specifies whether the port forwarding should be enabled.	Boolean choice
14	SSL_GROUP	Selects a group name for the portal (only for local authentication).	String, Max 32 characters and no ' or empty space or "

6.26 vpn sslvpn portal-layouts delete <*row_id*>

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

6.27 vpn sslvpn portforwarding appconfig add

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

6.28 vpn sslvpn portforwarding appconfig delete <*row_id*>

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

6.29 vpn sslvpn portforwarding hostconfig add

S.No	Command Name	Description	Type and Description
1	save	Saves portforwarding Host settings	
2	exit	Saves portforwarding Host settings and exit current mode	
3	cancel	To revert to the previous portforwarding Host settings.	

S.No	Command Name	Description	Type and Description
4	serverip	server ip address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	domain_name	domain name	String, Max 128 characters and no ' or empty space or "

6.30 vpn sslvpn portforwarding hostconfig delete *<row_id>*

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

6.31 vpn sslvpn resource add

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

6.32 vpn sslvpn resource configure add *<resource_name>*

S.No	Command Name	Description	Type and Description
1	*<resource_name>*	Adds an sslvpn resource object.	String, MAX 128 characters, ' is not supported;
2	save	Saves sslvpn resource object settings	
3	exit	Saves sslvpn resource settings, and exit current mode.	
4	cancel	To revert to previous sslvpn resource settings.	

S.No	Command Name	Description	Type and Description
5	object_type	object type	Sslvpn resource object type.
6	object_address	The object address of the resource object.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	mask_length	The mask length of the network.	number in range of 1 to 32
8	start_port	start port	Port number
9	end_port	end port	Port number
10	icmp	Enables this option to include ICMP traffic.	Source address type for users' ip policy.

6.33 vpn sslvpn resource configure delete *<row_id>*

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

6.34 vpn sslvpn resource delete *<row_id>*

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

6.35 vpn sslvpn policy add

S.No	Command Name	Description	Type and Description
1	save	Saves sslvpn policy settings	
2	exit	Saves sslvpn policy settings and exit current mode	
3	cancel	To revert to previous sslvpn policy settings.	
4	policy_type	Shows policy type.	Sslvpn policy type.
5	policy_owner	Shows policy owner	String
6	destination_objecttype	destination object type	Sslvpn policy destination type.
7	policy_name	policy name	String, character is not supported;

S.No	Command Name	Description	Type and Description
8	policy_address	policy address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
9	policy_masklength	policy masklength	number in range of 1 to 32
10	start_port	start port	Port number
11	end_port	end port	Port number
12	service_type	service type	sslvpn resource
13	resource_name	resource name	String, MAX 128 characters, ' is not supported;
14	policy_permission	This can be either Permit or Deny.	sslvpn policy type
15	icmp	Enables this option to include ICMP traffic.	source address type for users ip policy

6.36 vpn sslvpn policy edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Edits an sslvpn policy	Unsigned integer
2	save	Saves sslvpn policy settings	
3	exit	Saves sslvpn policy settings, and exit current mode	
4	cancel	To revert to previous sslvpn policy settings.	
5	policy_address	Enter the IP Address to which the SSL VPN Policy needs to be applied.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	policy_masklength	Enter the subnet mask for the above IP address.	number in range of 1 to 32
7	start_port	Start port.	Port number
8	end_port	End port.	Port number
9	resource_name	resource name	String, MAX 128 characters, ' is not supported.
10	policy_permission	Chooses either Permit or Deny for this policy.	Sslvpn policy type.
11	icmp	Enables this option to include ICMP traffic.	Source address type for users ip policy.

6.37 vpn sslvpn policy delete *<row_id>*

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

6.38 vpn sslvpn client

S.No	Command Name	Description	Type and Description
1	save	Saves sslvpn client settings	
2	exit	Saves sslvpn client settings and exit current mode	
3	cancel	To revert to previous sslvpn client settings.	
4	enable_fulltunnel	Enables full tunnel.	Boolean choice
5	dns_suffix	Sets the DNS Suffix for this client.	String
6	primary_dns	Sets the primary DNS Server for this client.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
7	secondary_dns	Sets the secondary DNS Server for this client.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	begin_clientaddress	Sets the first IP address of the IP address range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
9	end_clientaddress	Sets the last IP address of the IP address range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
10	lcp_timeout	This setting is to determine the wait time for a SSL VPN tunnel negotiation attempts.	Unsigned integer

6.39 vpn sslvpn route add

S.No	Command Name	Description	Type and Description
1	save	Saves sslvpn route settings	
2	exit	Saves sslvpn route settings, and exits current mode.	
3	cancel	To revert to previous sslvpn route settings.	

S.No	Command Name	Description	Type and Description
4	destination_network	destination network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
5	subnet_mask	subnet mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

6.40 vpn sslvpn route delete <*row_id*>

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

6.41 vpn ipsec policy configure <*name*>

S.No	Command Name	Description	Type and Description
1	*<name>*	vpn policy configuration mode	String
2	save	Saves vpn policy configuration settings.	
3	cancel	To revert to previous vpn policy configuration settings.	
4	exit	Saves vpn policy configuration settings, and exits 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_select_local _gateway	Setting local gateway for the vpn policy.	VPN gateway.
9	general_remote_end _point_type	Sets mode to IP address or Internet Name/FQDN of the remote gateway or client PC.	Vpn remote end point type.
10	general_remote_end _point	The IP address or Internet Name/FQDN of the remote gateway or client PC.	
11	general_remote_end _point ip_address	The IP address of the remote gateway or client PC.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6.

S.No	Command Name	Description	Type and Description
12	general_remote_end_point fqdn	The IP address or Internet Name/FQDN of the remote gateway or client PC.	String.
13	general_enable_mode_config	Enables/disables mode config which is similar to DHCP and is used to assign IP addresses to remote VPN clients.	Boolean choice.
14	general_enable_netbios	Enables/disables this to allow NetBIOS broadcasts to travel over the VPN tunnel.	Boolean choice.
15	general_enable_rollover	Enables this to allow the VPN to rollover when WAN Mode is set to Auto Rollover on the WAN Mode page.	Boolean choice
16	general_protocol	Setting protocol esp or ah.	IPsec VPN Protocol
17	general_enable_dhcp	Enables/disables dhcp.	Boolean choice
18	general_redundant_vpn_gateway	Enables/disables Redundant vpn gateway.	Boolean choice
19	general_backup_policy_name	Backup policy name.	String
20	general_failback_time	Failback time to switch from back-up to primary.	Unsigned integer
21	general_local_network_type	Selects the IP addresses on the local side that will be part of the tunnel. This can be either a single IP address, several IP addresses in a range, an entire subnet, or any IP address that wants to connect.	Vpn network type
22	general_local_start_address	IP address from where the range needs to begin.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
23	general_local_end_address	IP address where the range needs to end.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6
24	general_local_subnet_mask	Enter the Subnet Mask of the network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
25	general_local_prefix_length	Prefix length of the ipv6 subnet used.	IPv6 Prefix length

S.No	Command Name	Description	Type and Description
26	general_remote_network_type	Selects the IP addresses on the remote side that will be part of the tunnel. This can be either a single IP address, several IP addresses in a range, an entire subnet, or any IP address that wants to connect.	Vpn network type.
27	general_remote_start_address	IP address from where the range needs to begin.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6.
28	general_remote_end_address	IP address where the range needs to end.	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6.
29	general_remote_subnet_mask	Subnet mask of the subnet used.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
30	general_remote_prefix_length	Prefix length of the ipv6 subnet used.	IPv6 Prefix length.
31	general_enable_keepalive	Enables/disables keepalive	Boolean choice.
32	general_keepalive_sourceip	keepalive sourceip	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6.
33	general_keepalive_destinationip	keepalive destinationip	IPV4 or IPv6 address depending upon protocol selected IPV4 or IPV6.
34	general_keepalive_detection_period	Router sends ping packets periodically at regular intervals of time which is specified by the user.	Keepalive detection period in seconds.
35	general_keepalive_failure_count	Keepalive failure count of the specified number of consecutive packets for which the acknowledgement is not received.	Keepalive failure count.
36	general_l2tp_mode	Setting l2tp mode as None(0) or Client(1) or Gateway(2).	IPsec L2tp Mode.
37	manual_spi_in	Takes a hexadecimal value between 3 and 8 characters.	Takes a hexadecimal value between 3 and 8 characters.

S.No	Command Name	Description	Type and Description
38	manual_spi_out	Takes a hexadecimal value between 3 and 8 characters.	Takes a hexadecimal value between 3 and 8 characters.
39	manual_encryption_algorithm	The algorithm used to encrypt the data.	Vpn encryption algorithm.
40	manual_key_length	The key length for the algorithm.	Unsigned integer.
41	manual_encryption_key_in	Encryption key of the inbound policy. The length of the key depends on the algorithm chosen	String
42	manual_encryption_key_out	Encryption key of the outbound policy. The length of the key depends on the algorithm chosen.	String
43	manual_authentication_algorithm	Algorithm used to verify the integrity of the data.	Vpn authentication algorithm.
44	manual_authentication_key_in	This is the integrity key (for ESP with Integrity-mode) for the inbound policy and depends on the algorithm chosen.	String
45	manual_authentication_key_out	This is the integrity key (for ESP with Integrity-mode) for the outbound policy and depends on the algorithm chosen.	String
46	auto_phase1_exchange_mode	Setting IKE exchange Mode.	VPN Exchange Mode
47	auto_phase1_enable_nat_traversal	Enabling/Disabling Nat traversal.	Boolean choice
48	auto_phase1_nat_keepalive_frequecy	Setting IKE nat alive frequency.	Unsigned integer
49	auto_phase1_local_identtype	Setting IKE local identifier type.	IPsec VPN IKE local identifier type.
50	auto_phase1_direction_type	Setting IKE direction type.	IPsec VPN IKE direction Mode.
51	auto_phase1_local_identifier	Setting IKE local identifier.	String
52	auto_phase1_remote_identtype	Setting IKE remote identifier.	IPsec VPN IKE local identifier type.
53	auto_phase1_remote_identifier	Setting IKE remote identifier.	String
54	auto_phase1_encryption_algorithm	Setting IKE encryption algorithm.	

S.No	Command Name	Description	Type and Description
55	auto_phase1_encryption_algorithm DES	Setting IKE encryption algorithm.	
56	auto_phase1_encryption_algorithm DES enable_DES	Enables DES encryption algorithm.	Boolean choice
57	auto_phase1_encryption_algorithm 3DES	Setting IKE encryption algorithm.	
58	auto_phase1_encryption_algorithm 3DES enable_3DES *<3des>*	Enables 3DES encryption algorithm.	Boolean choice
59	auto_phase1_encryption_algorithm AES-128	Setting IKE encryption algorithm.	
60	auto_phase1_encryption_algorithm AES-128 enable_AES-128	Enables AES-128 encryption algorithm.	Boolean choice
61	auto_phase1_encryption_algorithm AES-192	Setting IKE encryption algorithm.	
62	auto_phase1_encryption_algorithm AES-192 enable_AES-192	Enables AES-192 encryption algorithm.	Boolean choice
63	auto_phase1_encryption_algorithm AES-256	Setting IKE encryption algorithm.	
64	auto_phase1_encryption_algorithm AES-256 enable_AES-256	Enables AES-256 encryption algorithm	Boolean choice
65	auto_phase1_encryption_algorithm BLOWFISH	Setting IKE encryption algorithm.	
66	auto_phase1_encryption_algorithm BLOWFISH enable_BLOWFISH	Enables BLOWFISH encryption algorithm.	Boolean choice
67	auto_phase1_encryption_algorithm BLOWFISH keylength	Enter BLOWFISH keylength.	Unsigned integer

S.No	Command Name	Description	Type and Description
68	auto_phase1_encryption_algorithm CAST128	Setting IKE encryption algorithm.	
69	auto_phase1_encryption_algorithm CAST128 enable_CAST128	Enables CAST128 encryption algorithm.	Boolean choice
70	auto_phase1_encryption_algorithm CAST128 keylength	Enter CAST128 keylength.	Unsigned integer
71	auto_phase1_auth_algorithm	Setting IKE authentication algorithm.	
72	auto_phase1_auth_algorithm MD5	Setting IKE authentication algorithm.	
73	auto_phase1_auth_algorithm MD5 enable_MD5	Enables MD5 authentication algorithm.	Boolean choice
74	auto_phase1_auth_algorithm SHA1	Setting IKE authentication algorithm.	
75	auto_phase1_auth_algorithm SHA1 enable_SHA1	Enables SHA1 authentication algorithm.	Boolean choice
76	auto_phase1_auth_algorithm SHA2-256	Setting IKE authentication algorithm.	
77	auto_phase1_auth_algorithm SHA2-256 enable_SHA2-256	Enables SHA2-256 authentication algorithm.	Boolean choice
78	auto_phase1_auth_algorithm SHA2-384	Setting IKE authentication algorithm.	
79	auto_phase1_auth_algorithm SHA2-384 enable_SHA2-384	Enables SHA2-384 authentication algorithm.	Boolean choice
80	auto_phase1_auth_algorithm SHA2-512	Setting IKE authentication algorithm.	
81	auto_phase1_auth_algorithm SHA2-512 enable_SHA2-512	Enables SHA2-512 authentication algorithm.	Boolean choice
82	auto_phase1_auth_method	Setting IKE authentication algorithm method.	IPsec VPN IKE authentication algorithm method.
83	auto_phase1_dh_group	Setting IKE Diffie-Hellman (DH) Group.	IPsec VPN IKE Diffie-Hellman (DH) Group type.
84	auto_phase1_sa_lifetime	Setting IKE SA lifetime in seconds.	Unsigned integer.
85	auto_phase1_pre_shared_key	Setting IKE pre shared key.	String

S.No	Command Name	Description	Type and Description
86	auto_phase1_enable_dead_peer_detection	Enabling/Disabling dead peer detection.	Boolean choice
87	auto_phase1_detection_period	Setting dead peer detection time period.	Unsigned integer
88	auto_phase1_reconnect_failure_count	Setting dead peer detection failure count.	Unsigned integer
89	auto_phase1_extended_authentication	Setting extended authentication method.	IPsec VPN IKE extended authentication method.
90	auto_phase1_authentication_type	Setting extended authentication type.	IPsec VPN IKE extended authentication method.
91	auto_phase1_xauth_username	Username for extended authentication.	String
92	auto_phase1_xauth_password	Password for extended authentication.	String
93	auto_phase2_sa_lifetime	Vpn auto policy phase2 configure.	
94	auto_phase2_sa_lifetime seconds	Setting IKE SA lifetime in seconds.	Unsigned integer
95	auto_phase2_sa_lifetime bytes	Setting IKE SA lifetime in bytes.	Unsigned integer
96	auto_phase2_encryption_algorithm	Setting IKE encryption algorithm.	
97	auto_phase2_encryption_algorithm DES	Setting IKE encryption algorithm.	
98	auto_phase2_encryption_algorithm DES enable_DES	Enables DES encryption algorithm.	Boolean choice
99	auto_phase2_encryption_algorithm 3DES	Setting IKE encryption algorithm.	
100	auto_phase2_encryption_algorithm 3DES enable_3DES *<3des>*	Enables 3DES encryption algorithm.	Boolean choice
101	auto_phase2_encryption_algorithm AES-128	Setting IKE encryption algorithm.	
102	auto_phase2_encryption_algorithm AES-128 enable_AES-128	Enables AES-128 encryption algorithm.	Boolean choice

S.No	Command Name	Description	Type and Description
103	auto_phase2_encryption_algorithm AES-192	Setting IKE encryption algorithm.	
104	auto_phase2_encryption_algorithm AES-192 enable_AES-192	Enables AES-192 encryption algorithm.	Boolean choice
105	auto_phase2_encryption_algorithm AES-256	Setting IKE encryption algorithm.	
106	auto_phase2_encryption_algorithm AES-256 enable_AES-256	Enables AES-256 encryption algorithm.	Boolean choice
107	auto_phase2_encryption_algorithm TWOFISH-128	Setting IKE encryption algorithm.	
108	auto_phase2_encryption_algorithm TWOFISH-128 enable_TWOFISH-128	Enables TWOFISH-128 encryption algorithm.	Boolean choice
109	auto_phase2_encryption_algorithm TWOFISH-192	Setting IKE encryption algorithm.	
110	auto_phase2_encryption_algorithm TWOFISH-192 enable_TWOFISH-192	Enables TWOFISH-192 encryption algorithm.	Boolean choice
111	auto_phase2_encryption_algorithm TWOFISH-256	Setting IKE encryption algorithm.	
112	auto_phase2_encryption_algorithm TWOFISH-256 enable_TWOFISH-256	Enables TWOFISH-256 encryption algorithm.	Boolean choice
113	auto_phase2_encryption_algorithm BLOWFISH	Setting IKE encryption algorithm.	
114	auto_phase2_encryption_algorithm BLOWFISH enable_BLOWFISH	Enables BLOWFISH encryption algorithm.	Boolean choice

S.No	Command Name	Description	Type and Description
115	auto_phase2_encryption_algorithm BLOWFISH keylength	Enters BLOWFISH keylength.	Unsigned integer
116	auto_phase2_encryption_algorithm CAST128	Setting IKE encryption algorithm.	
117	auto_phase2_encryption_algorithm CAST128 enable_CAST128	Enables CAST128 encryption algorithm.	Boolean choice
118	auto_phase2_encryption_algorithm CAST128 keylength	Enter CAST128 keylength.	Unsigned integer
119	auto_phase2_auth_algorithm	Setting IKE authentication algorithm.	
120	auto_phase2_auth_algorithm MD5	Setting IKE authentication algorithm.	
121	auto_phase2_auth_algorithm MD5 enable_MD5	Enables MD5 authentication algorithm.	Boolean choice
122	auto_phase2_auth_algorithm SHA1	Setting IKE authentication algorithm.	
123	auto_phase2_auth_algorithm SHA1 enable_SHA1	Enables SHA1 authentication algorithm.	Boolean choice
124	auto_phase2_auth_algorithm SHA2-256	Setting IKE authentication algorithm.	
125	auto_phase2_auth_algorithm SHA2-256 enable_SHA2-256	Enables SHA2-256 authentication algorithm.	Boolean choice
126	auto_phase2_auth_algorithm SHA2-384	Setting IKE authentication algorithm.	
127	auto_phase2_auth_algorithm SHA2-384 enable_SHA2-384	Enables SHA2-384 authentication algorithm.	Boolean choice
128	auto_phase2_auth_algorithm SHA2-224	Setting IKE authentication algorithm.	
129	auto_phase2_auth_algorithm SHA2-224 enable_SHA2-224	Enables SHA2-224 authentication algorithm.	Boolean choice
130	auto_phase2_auth_algorithm SHA2-512	Setting IKE authentication algorithm.	
131	auto_phase2_auth_algorithm SHA2-512 enable_SHA2-512	Enables SHA2-512 authentication algorithm.	Boolean choice

S.No	Command Name	Description	Type and Description
132	auto_phase2_enable_pfskeygroup	Enables/DIsables PFS key group.	Boolean choice
133	auto_phase2_dh_group	Setting IKE Diffie-Hellman (DH) Group.	IPsec VPN IKE Diffie-Hellman (DH) Group type

6.42 vpn ipsec dhcp configure

S.No	Command Name	Description	Type and Description
1	save	Saves vpn ipsec dhcp configuration settings.	
2	cancel	To revert to the previous vpn ipsec dhcp configuration settings.	
3	exit	Saves vpn ipsec dhcp configuration settings and exits current mode.	
4	start_address	Setting ipsec dhcp start address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	end_address	Setting ipsec dhcp end address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	subnet_mask	Setting ipsec dhcp subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

6.43 vpn ipsec policy enable <*name*>

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

6.44 vpn ipsec policy disable <*name*>

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

6.45 vpn ipsec policy delete <*name*>

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

6.46 vpn ipsec policy connect <*name*>

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

6.47 vpn ipsec policy drop <*name*>

S.No	Command Name	Description	Type and Description
1	*<name>*	Drops/Disconnects a vpn tunnel	String

Chapter 7. Configuration commands under branch DOT11

7.1 dot11 profile add *<profile_name>*

S.No	Command Name	Description	Type and Description
1	*<profile_name>*	802.11 profile configuration mode.	String
2	save	Saves profile configuration settings.	
3	exit	Saves profile configuration settings and exit current mode.	
4	ssid	Sets the 802.11 profile SSID.	String
5	broadcast-ssid	Enables or Disables SSID broadcast.	Boolean choice
6	security_type	Sets the profile security type.	802.11 Security Types
7	radio_mode	Sets the profile radio mode.	Dot11 Radio band
8	wep	Sets profile WEP options.	
9	wep authentication	Sets WEP authentication type.	WEP Authentication Types
10	wep encryption	Sets WEP encryption type.	WEP Encryption Types
11	wep key	Sets WEP key. Not required if passphrase is set.	WEP key index type (1-4) String
12	wep passphrase	Sets WEP passphrase to generate WEP key from.	WEP key index type (1-4) String
13	wpa	Sets the WPA options.	
14	wpa authentication	Sets WPA authentication type.	WPA Authentication Types
15	wpa encryption	Sets WPA encryption type.	WPA Encryption Types
16	wpa wpa-password	WPA Password. Needed only if authentication is PSK	String

7.2 dot11 profile edit *<profile_name>*

S.No	Command Name	Description	Type and Description
1	*<profile_name>*	802.11 profile configuration mode.	String

S.No	Command Name	Description	Type and Description
2	save	Saves profile configuration settings.	
3	exit	Saves profile configuration settings, and exit current mode.	
4	ssid	Sets the 802.11 profile SSID.	String
5	broadcast-ssid	Enables or DisablesSSID broadcast.	Boolean choice
6	security_type	Sets the profile security type.	802.11 Security Types
7	radio_mode	Sets the profile radio mode.	Dot11 Radio band
8	wep	Sets the profile WEP options.	
9	wep authentication	Sets the WEP authentication type.	WEP Authentication Types
10	wep encryption	Sets the WEP encryption type.	WEP Encryption Types
11	wep key	Sets the WEP key. Not required if passphrase is set.	WEP key index type (1-4) String
12	wep passphrase	Sets the WEP passphrase to generate WEP key from.	WEP key index type (1-4) String
13	wpa	Sets the WPA options.	
14	wpa authentication	Sets the WPA authentication type.	WPA Authentication Types
15	wpa encryption	Sets the WPA encryption type.	WPA Encryption Types
16	wpa wpa-password	WPA Password. Needed only if authentication is PSK	String

7.3 dot11 wmm edit *<profile_name>*

S.No	Command Name	Description	Type and Description
1	<profile_name>	The name of the profile to which service is being added will be displayed here. 802.11 wmm configuration mode.	String
2	save	Saves wmm configuration settings.	

S.No	Command Name	Description	Type and Description
3	exit	Saves wmm configuration settings, and exit current mode.	
4	enable	Enables/Disables the 802.11 profile wmm.	Boolean choice
5	default_class	Choose among "Background", "Best Effort", "video", "Voice". This class of service is used for the traffic for whose IP DSCP/TOS value is set to "Default" in IP TOS/DiffServ Mapping table.	Dot11 WMM class
6	dscp_0	Selects class of ip dscp.	Dot11 WMM class
7	dscp_1	Selects class of ip dscp.	Dot11 WMM class
8	dscp_2	Selects class of ip dscp.	Dot11 WMM class
9	dscp_3	Selects class of ip dscp.	Dot11 WMM class
10	dscp_4	Selects class of ip dscp.	Dot11 WMM class
11	dscp_5	Selects class of ip dscp.	Dot11 WMM class
12	dscp_6	Selects class of ip dscp.	Dot11 WMM class
13	dscp_7	Selects class of ip dscp.	Dot11 WMM class
14	dscp_8	Selects class of ip dscp.	Dot11 WMM class
15	dscp_9	Selects class of ip dscp.	Dot11 WMM class
16	dscp_10	Selects class of ip dscp.	Dot11 WMM class
17	dscp_11	Selects class of ip dscp.	Dot11 WMM class
18	dscp_12	Selects class of ip dscp.	Dot11 WMM class
19	dscp_13	Selects class of ip dscp.	Dot11 WMM class
20	dscp_14	Selects class of ip dscp.	Dot11 WMM class
21	dscp_15	Selects class of ip dscp.	Dot11 WMM class
22	dscp_16	Selects class of ip dscp.	Dot11 WMM class
23	dscp_17	Selects class of ip dscp.	Dot11 WMM class
24	dscp_18	Selects class of ip dscp.	Dot11 WMM class
25	dscp_19	Selects class of ip dscp.	Dot11 WMM class
26	dscp_20	Selects class of ip dscp.	Dot11 WMM class
27	dscp_21	Selects class of ip dscp.	Dot11 WMM class
28	dscp_22	Selects class of ip dscp.	Dot11 WMM class
29	dscp_23	Selects class of ip dscp.	Dot11 WMM class
30	dscp_24	Selects class of ip dscp.	Dot11 WMM class
31	dscp_25	Selects class of ip dscp.	Dot11 WMM class
32	dscp_26	Selects class of ip dscp.	Dot11 WMM class
33	dscp_27	Selects class of ip dscp.	Dot11 WMM class
34	dscp_28	Selects class of ip dscp.	Dot11 WMM class

S.No	Command Name	Description	Type and Description
35	dscp_29	Selects class of ip dscp.	Dot11 WMM class
36	dscp_30	Selects class of ip dscp.	Dot11 WMM class
37	dscp_31	Selects class of ip dscp.	Dot11 WMM class
38	dscp_32	Selects class of ip dscp.	Dot11 WMM class
39	dscp_33	Selects class of ip dscp.	Dot11 WMM class
40	dscp_34	Selects class of ip dscp.	Dot11 WMM class
41	dscp_35	Selects class of ip dscp.	Dot11 WMM class
42	dscp_36	Selects class of ip dscp.	Dot11 WMM class
43	dscp_37	Selects class of ip dscp.	Dot11 WMM class
44	dscp_38	Selects class of ip dscp.	Dot11 WMM class
45	dscp_39	Selects class of ip dscp.	Dot11 WMM class
46	dscp_40	Selects class of ip dscp.	Dot11 WMM class
47	dscp_41	Selects class of ip dscp.	Dot11 WMM class
48	dscp_42	Selects class of ip dscp.	Dot11 WMM class
49	dscp_43	Selects class of ip dscp.	Dot11 WMM class
50	dscp_44	Selects class of ip dscp.	Dot11 WMM class
51	dscp_45	Selects class of ip dscp.	Dot11 WMM class
52	dscp_46	Selects class of ip dscp.	Dot11 WMM class
53	dscp_47	Selects class of ip dscp.	Dot11 WMM class
54	dscp_48	Selects class of ip dscp.	Dot11 WMM class
55	dscp_49	Selects class of ip dscp.	Dot11 WMM class
56	dscp_50	Selects class of ip dscp.	Dot11 WMM class
57	dscp_51	Selects class of ip dscp.	Dot11 WMM class
58	dscp_52	Selects class of ip dscp.	Dot11 WMM class
59	dscp_53	Selects class of ip dscp.	Dot11 WMM class
60	dscp_54	Selects class of ip dscp.	Dot11 WMM class
61	dscp_55	Selects class of ip dscp.	Dot11 WMM class
62	dscp_56	Selects class of ip dscp.	Dot11 WMM class
63	dscp_57	Selects class of ip dscp.	Dot11 WMM class
64	dscp_58	Selects class of ip dscp.	Dot11 WMM class
65	dscp_59	Selects class of ip dscp.	Dot11 WMM class
66	dscp_60	Selects class of ip dscp.	Dot11 WMM class
67	dscp_61	Selects class of ip dscp.	Dot11 WMM class
68	dscp_62	Selects class of ip dscp.	Dot11 WMM class
69	dscp_63	Selects class of ip dscp.	Dot11 WMM class

.

7.4 dot11 radius configure

S.No	Command Name	Description	Type and Description
1	save	Saves radius configuration settings.	

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

7.5 dot11 profile delete <*profile_name*>

S.No	Command Name	Description	Type and Description
1	*<profile_name>*	Deletes an 802.11 profile.	String

7.6 dot11 accesspoint add *<ap_name>*

S.No	Command Name	Description	Type and Description
1	*<ap_name>*	802.11 access point configuration mode.	String
2	save	Saves AP configuration settings.	
3	cancel	To revert to the previous AP configuration settings.	
4	exit	Saves AP configuration settings, and exit current mode.	
5	profile	Sets the 802.11 profile the AP will use.	String
6	wlan_partition	Enables or Disables wlan_partition.	Boolean choice
7	enable_active_time	Setting time.	Boolean choice
8	enable_schedule_control	Enables/disables Schedule Control.	Boolean choice
9	start	Setting the time limits.	
10	stop	Setting the time limits.	
11	start hour	Setting the time limits.	H(1-12) using 12 hour clock
12	stop hour	Setting the time limits.	H(1-12) using 12 hour clock
13	start minute	Setting the time limits.	minute in the format MM(00-59)
14	stop minute	Setting the time limits.	minute in the format MM(00-59)
15	start meridian	Setting the time limits.	Schedule Meridiem Types.
16	stop meridian	Setting the time limits.	Schedule Meridiem Types.

7.7 dot11 accesspoint edit *<ap_name>*

S.No	Command Name	Description	Type and Description
1	<ap_name>	802.11 access point configuration mode	String
2	save	Saves AP configuration settings.	
3	cancel	To revert to the previous AP configuration settings	
4	exit	Saves AP configuration settings, and exits current mode.	
5	profile	Sets the 802.11 profile the AP will use.	String

S.No	Command Name	Description	Type and Description
6	wlan_partition	Enables or Disables wlan_partition.	Boolean choice
7	enable_active_time	Setting time.	Boolean choice
8	enable_schedule_control	Enables/disables Schedule Control.	Boolean choice
9	start	Setting the time limits.	
10	stop	Setting the time limits.	
11	start hour	Setting the time limits.	H(1-12) using 12 hour clock
12	stop hour	Setting the time limits.	H(1-12) using 12 hour clock
13	start minute	Setting the time limits.	minute in the format MM(00-59)
14	stop minute	Setting the time limits.	minute in the format MM(00-59)
15	start meridian	Setting the time limits.	Schedule Meridiem Types.
16	stop meridian	Setting the time limits.	Schedule Meridiem Types.

7.8 dot11 accesspoint delete <*ap_name*>

S.No	Command Name	Description	Type and Description
1	*<ap_name>*	Deletes an 802.11 access point.	String

7.9 dot11 wds enable <*radio_no*>

S.No	Command Name	Description	Type and Description
1	*<radio_no>*	Enables wds.	Unsigned integer

7.10 dot11 wds disable <*radio_no*>

S.No	Command Name	Description	Type and Description
1	*<radio_no>*	Disables wds.	Unsigned integer

7.11 dot11 wds add_peer *<radio_no> <mac_addr>*

S.No	Command Name	Description	Type and Description
1	*<radio_no> <mac_addr>*	Adds peer mac address wds.	Unsigned integer MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

7.12 dot11 wds delete_peer *<radio_no> <mac_addr>*

S.No	Command Name	Description	Type and Description
1	*<radio_no> <mac_addr>*	Deletes peer mac address wds.	Unsigned integer MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

7.13 dot11 accesspoint disable *<ap_name>*

S.No	Command Name	Description	Type and Description
1	*<ap_name>*	Disables an 802.11 access point.	String

7.14 dot11 accesspoint enable *<ap_name>*

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

7.15 dot11 radio configure *<radio_no>*

S.No	Command Name	Description	Type and Description
1	*<radio_no>*	802.11 radio configuration mode.	Unsigned integer
2	save	Saves radio configuration settings.	
3	cancel	To revert to the previous radio configuration settings.	

S.No	Command Name	Description	Type and Description
4	exit	Saves radio configuration settings, and exit current mode.	
5	channel	Sets the channel used by radio.	Dot11 Radio Channels.
6	default-transmit-power	Sets the default transmit power for APs using this radio.	Dot11 Radio default transmit power.
7	operating_freqency	Sets the dot11 radio operating frequency.	Dot11 Radio operating frequency band
8	2.4mode	Sets the dot11 radio mode.	Dot11 Radio Mode
9	5mode	Sets the dot11 radio mode.	Dot11 Radio Mode
10	transmission_rate	Sets the Transmission Rate for the radio.	Dot11 Radio Transmission Rate
11	channel_spacing	Sets the channel spacing for the radio.	Radio Channel Spacing.
12	control_side_band	Sets the contol band for radio.	Dot11 Radio control band

7.16 dot11 radio advanced configure *<radio_no>*

S.No	Command Name	Description	Type and Description
1	*<radio_no>*	802.11 AP advanced configuration mode.	Unsigned integer
2	save	Saves advanced AP configuration settings.	
3	cancel	To revert to the previous advanced AP configuration settings.	
4	exit	Saves advanced AP configuration settings and exit current mode.	
5	beacon_interval	Sets the time between beacon transmissions (in milliseconds).	Dot11 BEACON Interval.
6	dtim_interval	Sets the interval between delivery traffic indication messages.	Dot11 Dtim Interval.
7	rts_threshold	Sets the Request to Send (RTS) threshold.	Dot11 Rts thresold Interval.
8	fragmentation_threshold	Sets the maximum length of the frame.	Dot11 Fragmentation Interval.

S.No	Command Name	Description	Type and Description
9	preamble_mode	Sets the 802.11b preamble type to be prepended to every frame	802.11b Preamble Types.
10	protection_mode	Enables/disables RTS/CTS handshake before packet transmission.	RTSCTS Protection mode.
11	short_retry_limit	Sets the retry limit for frame retransmission on transmission failure.	802.11 Retry Limit.
12	long_retry_limit	Sets the retry limit for frame retransmission on transmission failure.	802.11 Retry Limit.
13	power_save_enable	Enables/Disables power save mode.	Boolean choice.
14	tx_antennas	Sets the no of transmit antennas to use.	Dot11 Antenna No.
15	rx_antennas	Sets the no of receive antennas to use.	Dot11 Antenna No.
16	ampdu_enable	Enables/Disables ampdu.	Boolean choice.

7.17 dot11 accesspoint wps configure

S.No	Command Name	Description	Type and Description
1	save	Saves WPS configuration settings.	
2	cancel	To revert to the previous WPS configuration settings	
3	exit	Saves WPS configuration settings, and exit current mode.	
4	access_point	Access point.	String.
5	wps_status	WPS status.	WPS status.
6	configure_via_pin	Configures WPS via PIN.	Boolean choice.
7	configure_via_pbc	Configures WPS via PBC.	Boolean choice.
8	station_pin	Sets the PIN for WPS config.	String.

7.18 dot11 accesspoint ACL configure *<ap_name>*

S.No	Command Name	Description	Type and Description
1	*<ap_name>*	802.11 AP ACL configuration mode.	String

S.No	Command Name	Description	Type and Description
2	save	Saves AP ACL configuration settings.	
3	cancel	To revert to the previous AP ACL configuration settings.	
4	exit	Saves the AP ACL configuration settings, and exit current mode.	
5	acl_policy	Sets the accesspoint ACL Policy.	Accesspoint ACL Policy type.
6	mac_address	Sets the accesspoint mac address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.

7.19 dot11 accesspoint acl delete_mac_address *<rowid>*

S.No	Command Name	Description	Type and Description
1	*<rowid>*	Deletes acl mac address entry.	Unsigned integer.

Chapter 8. Configuration commands under branch SYSTEM

8.1 System NT-Domain-Settings

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

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

8.2 system Active-Directory-Settings

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

S.No	Command Name	Description	Type and Description
13	first_admin_passwd	Sets the Active Directory first server admin password.	String
14	first_admin_hostname	Sets the Active Directory first server admin hostname.	String
15	second_admin_name	Sets the Active Directory second server admin name.	String
16	second_admin_passwd	Sets the Active Directory second server admin password.	String
17	second_admin_hostname	Sets the Active Directory second server admin hostname.	String
18	third_admin_name	Sets the Active Directory third server admin name.	String
19	third_admin_passwd	Sets the Active Directory third server admin password.	String
20	third_admin_hostname	Sets the Active Directory third server admin hostname.	String
21	serverCheck	Checks the reachability of configured servers.	

8.3 system LDAP_Settings

S.No	Command Name	Description	Type and Description
1	save	Saves LDAP configuration settings.	
2	exit	Saves LDAP configuration settings and exit.	
3	cancel	To revert to the previous configuration settings.	
4	Authentication_Server_1	Sets the primary server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
5	Authentication_Server_2	Sets the second alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
6	Authentication_Server_3	Sets the third alternative server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
7	LDAP_Base_DN	Sets the LDAP Base DN.	String
8	Second_LDAP_Base_DN	Sets the second alternative LDAP Base DN.	String
9	Third_LDAP_Base_DN	Sets the Third alternative LDAP Base DN.	String
10	LDAPAttribute1	Sets the LDAP Attribute 1.	String
11	LDAPAttribute2	Sets the LDAP Attribute 2.	String
12	LDAPAttribute3	Sets the LDAP Attribute 3.	String
13	LDAPAttribute4	Sets the LDAP Attribute 4.	String
14	timeout	Sets the LDAP server connection timeout.	Unsigned integer
15	retries	Sets the LDAP server connection retry attempts.	Unsigned integer
16	first_admin_name	Sets the LDAP first server admin name.	String
17	first_admin_passwd	Sets the LDAP first server admin password.	String
18	second_admin_name	Sets the LDAP second server admin name.	String
19	second_admin_passwd	Sets the LDAP second server admin password.	String
20	third_admin_name	Sets the LDAP third server admin name.	String
21	third_admin_passwd	Sets the LDAP third server admin password.	String
22	serverCheck	Checks the reachability of configured servers.	

8.4 system POP3_Settings POP3_Server_Configuration

S.No	Command Name	Description	Type and Description
1	save	Saves POP3 configuration settings.	
2	exit	Saves POP3 configuration settings and exit.	
3	cancel	To revert to the previous configuration settings.	
4	Authentication_Server_1	Sets the primary server.	String
5	Authentication_Server_2	Sets the secondary server.	String

S.No	Command Name	Description	Type and Description
6	Authentication_Server_3	Sets the optional server.	String
7	Authentication_Port_1	Sets the port for primary server.	Port number
8	Authentication_Port_2	Sets the port for secondary server.	Port number
9	Authentication_Port_3	Sets the port for optional server.	Port number
10	SSL_Enable_1	Enables the SSL for primary server.	Boolean choice
11	SSL_Enable_2	Enables the SSL for secondary server.	Boolean choice
12	SSL_Enable_3	Enables the SSL for optional server.	Boolean choice
13	CA_File_1	CAFILE for primary server.	String
14	CA_File_2	CAFILE for secondary server.	String
15	CA_File_3	CAFILE for optional server.	String
16	serverCheck	Checks the reachability of configured servers.	

8.5 system POP3_Settings POP3_Trusted_CA

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

8.6 system logging ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Saves logging configuration settings.	
2	exit	Saves logging configuration settings and exit current mode.	
3	cancel	To revert to the previous logging configuration settings.	

S.No	Command Name	Description	Type and Description
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

8.7 system logging facility configure *<facility>*

S.No	Command Name	Description	Type and Description
1	*<facility>*	System logging facility configuration mode.	Logging Facility Type.
2	save	Saves log Facility configuration settings.	
3	exit	Saves log facility configuration settings and exit current mode.	
4	cancel	To revert to the previous log Facility configuration settings.	
5	level_options_set	Sets level options. This command can run multiple times in this view to set different level options.	Logging Facility Type. Logging Level Options Type. Boolean choice.

8.8 system logging remote configure

S.No	Command Name	Description	Type and Description
1	save	Saves remote Logging configuration settings.	
2	exit	Saves remote logging configuration settings and exit current mode.	
3	cancel	To revert to the previous remote logging configuration settings.	
4	log_identifier	Sets the log identifier prefixed to both, e-mail and Syslog messages.	String
5	email_logs_enable	Sets whether or not system emails scheduled logs.	Boolean choice
6	email_server	Sets options for emailing of logs.	String
7	smtp_port	The SMTP port of the e-mail server.	Port number
8	return_email_address	Sets email address SMTP server replies are sent.	String
9	send_to_email_address	Sets email address where logs and alerts will be sent.	String
10	send_to_email_address2	Sets email address where logs and alerts will be sent.	String

S.No	Command Name	Description	Type and Description
11	send_to_email_address3	Sets email address where logs and alerts will be sent.	String
12	smtp_auth	Sets SMTP authentication details.	
13	smtp_auth type	Sets SMTP authentication types.	SMTP Authentication Types.
14	smtp_auth username	Sets SMTP authentication username (for plain and CRAM-MD5 auth).	String
15	smtp_auth password	Sets SMTP authentication password (for plain and CRAM-MD5 auth).	String
16	Tls_Enable	Enables Tls support (for plain and CRAM-MD5 auth).	Boolean choice
17	identd_from_smtp_server_enable	Enables/Diables to identd from smtp server.	Boolean choice
18	schedule	Sets schedule for sending log by email.	
19	schedule unit	Sets schedule unit.	Schedule Unit Types.
20	schedule day	Sets schedule day.	Schedule Day Types.
21	schedule time	Sets schedule time.	Schedule Time Units Types.
22	schedule meridiem	Sets schedule meridiem.	Schedule Meridiem Types.
23	syslog_server	syslog	
24	syslog_server server_name1	server1	
25	syslog_server server_name2	server2	
26	syslog_server server_name3	server3	
27	syslog_server server_name4	server4	
28	syslog_server server_name5	server5	
29	syslog_server server_name6	server6	
30	syslog_server server_name7	server7	
31	syslog_server server_name8	server8	
32	syslog_server server_name1 enable	Boolean Choice Y/N	Boolean choice

S.No	Command Name	Description	Type and Description
33	syslog_server server_name1 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
34	syslog_server server_name1 severity	Sets Syslog severity.	Syslog server severity types.
35	syslog_server server_name1 facility	Sets Syslog facility.	Syslog server facility ID types
36	syslog_server server_name2 enable	Boolean Choice Y/N.	Boolean choice
37	syslog_server server_name2 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
38	syslog_server server_name2 severity	Sets Syslog severity.	Syslog server severity types.
39	syslog_server server_name2 facility	Sets Syslog facility.	Syslog server facility ID types.
40	syslog_server server_name3 enable	Boolean Choice Y/N.	Boolean choice
41	syslog_server server_name3 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
42	syslog_server server_name3 severity	Sets Syslog severity.	Syslog server severity types.
43	syslog_server server_name3 facility	Sets Syslog facility.	Syslog server facility ID types.
44	syslog_server server_name4 enable	Boolean Choice Y/N	Boolean choice
45	syslog_server server_name4 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
46	syslog_server server_name4 severity	Sets Syslog severity.	Syslog server severity types.
47	syslog_server server_name4 facility	Sets Syslog facility.	Syslog server facility ID types.

S.No	Command Name	Description	Type and Description
48	syslog_server server_name5 enable	Boolean Choice Y/N.	Boolean choice
49	syslog_server server_name5 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
50	syslog_server server_name5 severity	Sets Syslog severity.	Syslog server severity types.
51	syslog_server server_name5 facility	Sets Syslog facility.	Syslog server facility ID types.
52	syslog_server server_name6 enable	Boolean Choice Y/N.	Boolean choice
53	syslog_server server_name6 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
54	syslog_server server_name6 severity	Sets Syslog severity.	Syslog server severity types.
55	syslog_server server_name6 facility	Sets Syslog facility.	Syslog server facility ID types.
56	syslog_server server_name7 enable	Boolean Choice Y/N.	Boolean choice
57	syslog_server server_name7 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
58	syslog_server server_name7 severity	Sets Syslog severity.	Syslog server severity types.
59	syslog_server server_name7 facility	Sets Syslog facility.	Syslog server facility ID types.
60	syslog_server server_name8 enable	Boolean Choice Y/N.	Boolean choice.
61	syslog_server server_name8 name	Sets Syslog server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
62	syslog_server server_name8 severity	Sets Syslog severity.	Syslog server severity types.

S.No	Command Name	Description	Type and Description
63	syslog_server server_name8 facility	Sets Syslog facility.	Syslog server facility ID types.

8.9 system logging ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Saves ipv6 logging configuration settings.	
2	exit	Saves ipv6 logging configuration settings, and exits current mode.	
3	cancel	To revert to the previous ipv6 logging configuration settings.	
4	lan_wan_accept_enable	Enasbles/Disables logging for the LAN to WAN Accept packets.	Boolean choice
5	lan_wan_drop_enable	Enables/Disables logging for the LAN to WAN Dropped packets.	Boolean choice
6	wan_lan_accept_enable	Enables/Disables logging for the WAN to LAN Accept packets.	Boolean choice
7	wan_lan_drop_enable	Enables/Disables logging for the WAN to LAN Dropped packets.	Boolean choice

8.10 system Radius-Settings

S.No	Command Name	Description	Type and Description
1	save	Saves RADIUS configuration settings.	
2	exit	Saves RADIUS configuration settings and exit current mode.	
3	cancel	To revert to the previous configuration settings	
4	primary-radius-server	Sets Primary RADIUS server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	secondary-radius-server	Sets Secondary RADIUS server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
6	optional-radius-server	Sets Optional RADIUS server IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	primary-server-authentication-port	Sets Primary RADIUS server port.	Port number
8	secondary-server-authentication-port	Sets Secondary RADIUS server port.	Port number
9	optional-server-authentication-port	Sets Optional RADIUS server port.	Port number
10	primary-server-secret	Sets Primary RADIUS server secret.	String
11	secondary-server-secret	Sets Secondary RADIUS server secret.	String
12	optional-server-secret	Sets Optional RADIUS server secret.	String
13	primary-server-timeout	Sets primary server connection timeout.	Radius server connection timeout in seconds
14	secondary-server-timeout	Sets secondary server connection timeout.	Radius server connection timeout in seconds
15	optional-server-timeout	Sets optional server connection timeout.	Radius server connection timeout in seconds
16	primary-server-retries	Sets primary server connection retry attempts.	Radius server retries attempts.
17	secondary-server-retries	Sets secondary server connection retry attempts.	Radius server retries attempts.
18	optional-server-retries	Sets optional server connection retry attempts.	Radius server retries attempts.
19	serverCheck	Checks the reachability of configured servers.	

8.11 system remote_management https configure

S.No	Command Name	Description	Type and Description
1	save	Saves access Management settings for https.	
2	exit	Saves access Management settings for https and exit current mode.	
3	cancel	To revert to the previous Remote Mgmt settings.	
4	enable	Enables/disables remote mgmt over https.	Boolean choice

S.No	Command Name	Description	Type and Description
5	type	Enables/disables remote mgmt over https.	Unsigned integer
6	from_address	Sets the starting IP in case of range, and the IP to be allowed access in case of granting access to a particular machine	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	end_address	Sets the Ending IP in case of range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	port	Sets the port you want to use for HTTP.	Unsigned integer
9	enable_remote_snmp	Enables/disables remote snmp.	Boolean choice
10	enable_remote_ssh	Enables/disables remote ssh.	Boolean choice

8.12 system remote_management telnet configure

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

8.13 system sessionSettings admin configure

S.No	Command Name	Description	Type and Description
1	save	Saves Configurable WAN settings.	
2	exit	Saves configurable settings and exit current mode.	
3	cancel	To revert to the previous Configurable Session settings settings.	
4	SessionTimeout	Enters the Session timeout for the admin group.	Idle timeout value for user.

8.14 system sessionSettings guest configure

S.No	Command Name	Description	Type and Description
1	save	Saves Configurable settings.	
2	exit	Saves configurable settings and exit current mode.	
3	cancel	To revert to the previous Configurable Session settings.	
4	SessionTimeout	Enters the Session timeout for the guest group.	Idle timeout value for user.

8.15 system snmp trap configure *<agent_ip>*

S.No	Command Name	Description	Type and Description
1	*<agent_ip>*	SNMP trap configuration mode.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
2	save	Saves SNMP trap configuration settings.	
3	exit	Saves SNMP trap configuration settings, and exit current mode.	
4	cancel	To revert to the previous snmp configuration settings.	
5	agent	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
6	snmp_version	Snmp Version v1/v2/v3	String

S.No	Command Name	Description	Type and Description
7	port	SNMP trap port the trap messages will be sent to.	Port number
8	community	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community.	String

8.16 system snmp trap delete *<agent_ip>*

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

8.17 system snmp users configure *<user>*

S.No	Command Name	Description	Type and Description
1	*<user>*	SNMP v3 User list configuration settings	snmpv3uers list user type
2	save	Saves SNMP trap configuration settings.	
3	exit	Saves SNMP v3 Users configuration settings and exit current mode.	
4	cancel	To revert to the previous SNMP v3 Users configuration settings.	
5	security_level	Authentication and privacy settings.	Snmp security level type for snmpv3users list.
6	authentication_algo	Selects either MD5 or SHA authentication.	Snmpv3uers list authentication algorithm type.
7	privacy_algorithm	DES-56 privacy is available for the authentication negotiation.	Snmpv3uers list privacy algorithm type.
8	authentication_password	Shared authentication password with the SNMPv3 user.	String
9	privacy_password	Shared privacy password with the SNMPv3 user.	String

8.18 system snmp sys configure

S.No	Command Name	Description	Type and Description
1	save	Saves SNMP system configuration settings.	
2	cancel	To revert to the previous snmp configuration settings.	
3	exit	Saves SNMP system configuration settings and exit current mode.	
4	sys-contact	Sets system contact information.	String, Max 32 characters and no ' or empty space or".
5	sys-location	Sets system location information.	String, Max 32 characters and no ' or empty space or".
6	sys-name	Sets system name information.	String, Max 32 characters and no ' or empty space or ".

8.19 system snmp access add

S.No	Command Name	Description	Type and Description
1	save	Saves SNMP access control configuration settings.	
2	exit	Saves SNMP access configuration settings and exit current mode.	
3	cancel	To revert to the previous snmp configuration settings.	
4	agent	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
5	subnet_mask	The network mask used to determine the list of allowed SNMP managers. To allow any IP on the network to manager the device enter 255.255.255.0. For a specific host, enter 255.255.255.255. To allow global access, enter 0.0.0.0.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
6	accessType	SNMP trap port the trap messages will be sent to.	String

S.No	Command Name	Description	Type and Description
7	community	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community	String

8.20 system snmp access edit *<rowid>*

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

8.21 system snmp access delete *<rowid>*

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

8.22 system switch_settings power_saving configure

S.No	Command Name	Description	Type and Description
1	save	Saves powerMode configuration settings.	
2	exit	Saves power mode configuration settings, and exit current mode.	
3	cancel	To revert to the previous content Filtering ower mode configuration settings.	
4	link_status	Enables/Disables Link status	Boolean choice
5	cable_length	Enables/Disables Cable Length	Boolean choice

8.23 system switch_settings jumbo_frame configure

S.No	Command Name	Description	Type and Description
1	save	Saves jumbo frame configuration settings.	
2	exit	Saves jumbo frame configuration settings and exit current mode.	
3	cancel	To revert to the previous jumbo frame configuration settings.	
4	jumbo_frame	Enables/Disables jumbo frame.	Boolean choice

8.24 system admin_setting configure

S.No	Command Name	Description	Type and Description
1	save	Saves system admin settings.	
2	exit	Saves configuration settings, and exit current mode.	
3	cancel	To revert to the previous admin configuration settings.	
4	System_name		String

8.25 system time configure

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

8.26 system traffic_meter configure

S.No	Command Name	Description	Type and Description
1	save	Saves traffic meter configuration settings.	
2	exit	Saves traffic meter configuration settings and exit current mode.	
3	cancel	To revert to the previous traffic meter configuration settings.	
4	enable	Enables/Disables the traffic meter status.	Boolean choice
5	limit_type	Sets traffic Limit Type 0(No limit), 1(Download only), 2(Both Directions).	traffic meter types
6	monthly_limit	Sets the monthly limit value of the traffic meter.	Unsigned integer
7	increase_limit_enable	Enables/Disables status of increase limit of the traffic meter option.	Boolean choice
8	increase_limit_by	Sets the value to increase limit of the traffic meter.	Unsigned integer
9	counter	Sets traffic counter as either specific time or restart counter now.	traffic counter type
10	time_hour	Sets hours for restart time.	HH(00-23) using 24 hour clock
11	time_minute	Sets minutes for restart time.	Minute in the format MM(00-59)
12	day_of_month	Sets day of month.	Calendar day of month
13	send_email_report	Enables/Disables send email report.	Boolean choice
14	block_type	Sets block Traffic type 0(block all traffic) 1(block all traffic except email).	Block traffic type.
15	send_email_alert	Enables/Disables send email alert.	Boolean choice

8.27 system usb usb1 configure

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

S.No	Command Name	Description	Type and Description
2	exit	Saves configurable WAN settings and exit current mode.	
3	cancel	To revert to the previous Configurable WAN settings settings.	
4	enable	Enables USB1	Boolean choice
5	printer_enable	Enables printer usb	Boolean choice
6	Storage_enable	Enables Storage USB	Boolean choice
7	usb_type	Selects the USB type 3G_USB_ADAPTOR/USB_Disc	usb device type

8.28 system usb usb2 configure

S.No	Command Name	Description	Type and Description
1	save	Saves USB1 Settings settings.	
2	exit	Saves USB2 settings and exit current mode.	
3	cancel	To revert to the previous Configurable WAN settings settings.	
4	enable	Enables USB2.	Boolean choice
5	printer_enable	Enables printer.	Boolean choice
6	Storage_enable	Enables USB2.	Boolean choice
7	usb_type	Selects the USB type 3G_USB_ADAPTOR/USB_Disc.	usb device type

8.29 system usb shareport_vlan configure *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	SharePort on vlan configuration.	Unsigned integer
2	save	Saves SharePort on vlan settings.	
3	exit	Saves shareport on vlan settings and exit current mode.	

S.No	Command Name	Description	Type and Description
4	cancel	To revert to the previous shareport on vlan settings.	
5	printer_sharing	Enables printer	Boolean choice
6	storage_sharing	Enables USB2	Boolean choice

8.30 system group add

S.No	Command Name	Description	Type and Description
1	save	Saves system group configuration settings.	
2	exit	Saves system group configuration settings and exit current mode.	
3	cancel	To revert to the previous system group configuration settings.	
4	groupname	Enter the Group Name here	String
5	description	Enter a brief description of the group here	String
6	Privilege_Type	Selects the privilege type for the group.	
7	Privilege_Type Admin	Adds ADMIN privilege to the group.	Boolean choice
8	Privilege_Type sslvpn	Adds sslvpn privilege to the group.	Boolean choice
9	Privilege_Type L2TP	Adds L2TP privilege to the group.	Boolean choice
10	Privilege_Type PPTP	Adds PPTP privilege to the group.	Boolean choice
11	Privilege_Type Xauth	Adds Xauth privilege to the group.	Boolean choice
12	Privilege_Type Guest	Adds Guest privilege to the group.	Boolean choice
13	Privilege_Type Captive_Portal	Adds captive portal privilege to the group.	Boolean choice
14	grouptimeOut	Enter the time out for the group.	Idle timeout value for user.

8.31 system group edit *<row_id>*

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

S.No	Command Name	Description	Type and Description
2	save	Saves system group configuration settings.	
3	exit	Saves system group configuration settings and exit current mode.	
4	cancel	To revert to the previous system group configuration settings.	
5	description	Enter a brief description of the group here.	String
6	grouptimeOut	Enter the new time out for the group.	Idle timeout value for user.

8.32 system group delete *<row_id>*

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

8.33 system users add

S.No	Command Name	Description	Type and Description
1	save	Saves system user configuration settings.	
2	exit	Saves system user configuration settings and exit current mode.	
3	cancel	To revert to the previous system user configuration settings.	
4	username	Enter the username here.	String
5	FirstName	Enter the user's first name here.	String
6	LastName	Enter the user's last name here.	String
7	password	Enter the password here.	String
8	password_confirm	Re-Enter the password here.	String
9	groupname	Enter the groupname here.	String
10	enable_change_password	Enables/Disables change password for captive portal user.	Boolean choice

8.34 system users edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	System users edit mode.	Unsigned integer
2	save	Saves system user configuration settings.	
3	exit	Saves system user configuration settings and exit current mode.	
4	cancel	To revert to the previous system user configuration settings.	
5	FirstName	Enter the user's first name here.	String
6	LastName	Enter the user's last name here.	String
7	change_password	Change user's password.	String String String
8	enable_change_password	Enables/Disables change password for captive portal user.	Boolean choice

8.35 system users delete *<row_id>*

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

8.36 system group groupaccesscontrol configure *<group_id>*

S.No	Command Name	Description	Type and Description
1	*<group_id>*	group access control configuration.	Unsigned integer
2	save	Saves group access control configuration settings.	
3	exit	Saves group access control configuration settings and exit current mode.	
4	cancel	To revert to the previous group access control configuration settings.	
5	deny_login	Denies login.	Boolean choice
6	deny_login_wan	Denies login wan.	Boolean choice

S.No	Command Name	Description	Type and Description
7	allow_login_from_defined_ips	Login from ip.	Boolean choice
8	allow_login_from_defined_browsers	Login from browser.	Boolean choice

8.37 system group access_control_browser add

S.No	Command Name	Description	Type and Description
1	save	Saves group access control browser configuration settings.	
2	exit	Saves group access control browser configuration settings and exit current mode.	
3	cancel	To revert to the previous group access control browser configuration settings.	
4	group_id	group id	Unsigned integer
5	browser_name	browser name	Supported browsers

8.38 system group access_control_browser delete *<row_id>*

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

8.39 system group access_control_ip add

S.No	Command Name	Description	Type and Description
1	save	Saves group access control ip configuration settings.	
2	exit	Saves group access control ip configuration settings and exit current mode.	

S.No	Command Name	Description	Type and Description
3	cancel	To revert to the previous group access control ip configuration settings.	
4	group_id	group id	Unsigned integer
5	address_type	address type	source address type for users ip policy
6	source_address	Sets the source address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	mask_length	Sets the source network mask length.	number in range of 1 to 32

8.40 system group access_control_ip delete *<row_id>*

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

Chapter 9. Configuration commands under branch UTIL

9.1 util system_check ping *<ip_address>*

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

9.2 util system_check dns_lookup *<dns>*

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

9.3 util system_check traceroute *<ip_address>*

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

9.4 util system_check capturePackets start *<interface>*

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

9.5 util system_check capturePackets download *<fileName> <ipAddr>*

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

9.6 util dbglog_download *<fileName> <ipAddr>*

S.No	Command Name	Description	Type and Description
1	*<fileName> <ipAddr>*	Downloads Dbglogs to the host machine	FileName string IP address

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

9.7 util usb_test *<ipAddr> <fileName>*

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

9.8 util firmware_upgrade <IpAddr> <FileName>

S.No	Command Name	Description	Type and Description
1	*<IpAddr> <FileName>*	To upgrade the firmware.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 String.

9.9 util enable_auto_backup *<status>*

S.No	Command Name	Description	Type and Description
1	*<status>*	Enables/Disables Auto Backup support.	Boolean choice.

9.10 util enable_config_encryp *<status>*

S.No	Command Name	Description	Type and Description
1	*<status>*	Enables/Disables Configuration encryption support.	Boolean choice

9.11 util watchdog_disable *<status>*

S.No	Command Name	Description	Type and Description
1	*<status>*	Disables/Enables watchdog timer.	Boolean choice

Chapter 10. Configuration commands under branch LICENSE

10.1 license list

S.No	Command Name	Description	Type and Description
1	list	Lists all licenses configured on the device.	
2	activate	Activates a license on the device.	

10.2 license activate *<activationKey>*

S.No	Command Name	Description	Type and Description
1	*<activationKey>*	Activates a license on the device.	Takes a string value that has only AtoZ, atoz and 0to9 characters only
2	list	Lists all licenses configured on the device.	
3	activate	Activates a license on the device.	

Chapter 11. Configuration commands under branch NET

11.1 net ipv6_tunnel six_to_four configure

S.No	Command Name	Description	Type and Description
1	save	Saves sixToFour Tunnel configuration settings.	
2	exit	Saves sixToFour Tunnel configuration settings, and exits current mode.	
3	cancel	To revert to the previous sixToFourTunnel configuration settings.	
4	automatic_tunneling_enable	Enables/disables automatic tunneling which will allow traffic from a LAN IPv6 network to be tunneled through a WAN IPv4 network to reach an IPV6 network.	Boolean choice

11.2 net bandwidth profile enable *<enable>*

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

11.3 net bandwidth profile add

S.No	Command Name	Description	Type and Description
1	save	Saves bandwidth profile configuration settings.	
2	exit	Saves bandwidth Profile configuration settings and exit current mode.	
3	cancel	To revert to the previous bandwidth Profile configuration settings.	
4	name	Unique Profile Name.	String
5	policytype	Policy Type, either Inbound or Outbound.	Bandwidth policy type.

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

11.4 net bandwidth profile edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	It allows to edit a bandwidth profile.	Unsigned integer
2	save	Saves bandwidth profile configuration settings.	
3	exit	Saves bandwidth Profile configuration settings and exit current mode.	
4	cancel	To revert to the previous bandwidth Profile configuration settings.	
5	name	Unique Profile Name.	String
6	policytype	Policy Type, either Inbound or Outbound.	Bandwidth policy type.
7	type	Profile Type, either Priority or Rate.	Bandwidth profile type.
8	priority	Select from Low, Medium or High if the profile type is priority.	Bandwidth priority type.
9	minimum_rate	Minimum Bandwidth provided by user.	Minimum bandwidth rate 0-Max bandwidth Kbps.
10	maximum_rate	Maximum Bandwidth provided by user.	Maximum bandwidth rate 100-100000 Kbps.

S.No	Command Name	Description	Type and Description
11	Interface	Enter WAN interface (WAN1/WAN2) for Outbound Policy and LAN/VLAN (Use show net bandwidth profile interface_list command to see list)interface for Inbound Bandwidth Profile.	String

11.5 net bandwidth profile delete *<row_id>*

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

11.6 net bandwidth traffic_selector add

S.No	Command Name	Description	Type and Description
1	save	Saves Traffic Selector configuration settings.	
2	exit	Saves Traffic Selector configuration settings and exit current mode.	
3	cancel	To revert to the previous Traffic Selector configuration settings.	
4	profile_name	Profile Name.	String
5	service_name	To see available services list by show command.	String
6	match_type	The match type can be IP or MAC Address.	Traffic selector match type.
7	ip_address	IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
8	subnet_mask	Subnet Mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
9	mac_address	MAC Address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
10	port_name	Port Name	Traffic selectors Port types.
11	vlan_id	Vlan ID	Unsigned integer.
12	access_point	Virtual Access Point Name	String.

11.7 net bandwidth traffic_selector edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	It allows to edit a traffic selector for a bandwidth profile.	Unsigned integer
2	save	Saves Traffic Selector configuration settings.	
3	exit	Saves Traffic Selector configuration settings and exit current mode.	
4	cancel	To revert to the previous Traffic Selector configuration settings.	
5	profile_name	Profile Name.	String
6	service_name	Sees available services list by show command	String
7	match_type	IP /MAC Address	Traffic selector match type.
8	ip_address	IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
9	subnet_mask	Subnet Mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
10	mac_address	MAC Address	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
11	port_name	Port Name	Traffic selectors Port types.
12	vlan_id	Vlan ID	Unsigned integer.
13	access_point	Virtual Access Point Name	String

11.8 net bandwidth traffic_selector delete *<row_id>*

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

11.9 net ddns wan1 configure

S.No	Command Name	Description	Type and Description
1	save	Saves DDNS configuration settings.	
2	exit	Saves DDNS configuration settings and exit current mode.	
3	cancel	To revert to the previous DDNS configuration settings.	
4	ddns_service	Enables or Disables Dyndns to provide Dynamic DNS service	Select the Ddns Service type.
5	hostname	Sets Hostname.	String, Max 64 characters and no ' or empty space or "
6	username	Sets username.	String, Max 64 characters and no ' or empty space or "
7	password	Sets Password.	String, Max 64 characters and no ' or empty space or "
8	time_update_enable	Sets Timeperiod as 30 days.	Boolean choice
9	wild_flag_enable	Enables/Disables using wild cards.	Boolean choice

11.10 net ddns wan2 configure

S.No	Command Name	Description	Type and Description
1	save	Saves DDNS configuration settings.	
2	exit	Saves DDNS configuration settings and exit current mode.	
3	cancel	To revert to the previous DDNS configuration settings.	
4	ddns_service	Enables or Disables Dyndns to provide Dynamic DNS service	Select the Ddns Service type.
5	hostname	Sets Hostname.	String, Max 64 characters and no ' or empty space or "
6	username	Sets username.	String, Max 64 characters and no ' or empty space or "
7	password	Sets Password.	String, Max 64 characters and no ' or empty space or "

S.No	Command Name	Description	Type and Description
8	time_update_enable	Sets Timeperiod as 30 days.	Boolean choice
9	wild_flag_enable	Enables/Disables using wild cards.	Boolean choice

11.11 net lan dhcp reserved_ip configure *<mac_address>*

S.No	Command Name	Description	Type and Description
1	*<mac_address>*	DHCP Reserved IPs add/edit mode.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF
2	save	Saves DHCP Reserved IPs configuration settings.	
3	exit	Saves DHCP Reserved IPs configuration settings, and exit current mode.	
4	cancel	To revert to the previous DHCP Reserved IPs configuration settings.	
5	ip_address	Sets IP Address to be reserved.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	computer_name	Specifies a unique name.	String
7	Association	Selects to Associate with IP / MAC Binding.	Boolean choice
8	log_dropped_packets	Specifies logging option for this rule.	Boolean choice

11.12 net lan dhcp reserved_ip delete *<mac_address>*

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

11.13 net dmz dhcp reserved_ip configure *<mac_address>*

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

11.14 net dmz dhcp reserved_ip delete *<mac_address>*

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

11.15 net ethernet configure *<interface_name>*

S.No	Command Name	Description	Type and Description
1	*<interface_name>*	Ethernet configuration mode.	String
2	save	Saves ethernet configuration settings.	
3	exit	Saves ethernet configuration settings, and exits current mode.	
4	cancel	To revert to the previous configuration settings.	
5	vlan-enable	Enables/Disables VLAN for this interface.	Boolean choice

S.No	Command Name	Description	Type and Description
6	native-vlan	Enables/Disables native VLAN status.	Boolean choice
7	vlanid	Sets VLAN Id.	Unsigned integer

11.16 net lan ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Saves LAN configuration settings.	
2	exit	Saves LAN configuration settings and exit current mode.	
3	cancel	To revert to the previous LAN configuration settings.	
4	static	Configures LAN Settings.	
5	static address	Sets system LAN IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	static subnet_mask	Sets system LAN subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	dhcp	Configures DHCP Settings.	
8	dhcp mode	Sets dhcp mode.	dhcpv4 modes
9	dhcp start_address	Sets dhcp servers start address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	dhcp end_address	Sets dhcp servers end address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	dhcp default_gw	Sets dhcp default gateway.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	dhcp primary_dns	Sets primary dns server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	dhcp secondary_dns	Sets secondary dns server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	dhcp wins_server	Sets Wins Server address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
15	dhcp lease_time	Sets system Lease Time.	Number in range of 1 to 262800.

S.No	Command Name	Description	Type and Description
16	dhcp domain_name	Sets dhcp domain name.	String, Max 256 characters and no ' or empty space or "
17	dhcp relay_gateway	Sets dhcp relays gateway address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
18	dns	Configures DNS Settings.	
19	dns host_name	Configures DNS Settings.	
20	dns host_name mapping	Configures DNS Host NameMapping.	
21	dns host_name mapping 1	Configures DNS Host NameMapping for 1st row.	
22	dns host_name mapping 2	Configures DNS Host NameMapping for 2nd Row.	
23	dns host_name mapping 3	Configures DNS Host NameMapping for 3rd row.	
24	dns host_name mapping 4	Configures DNS Host NameMapping for 4th row.	
25	dns host_name mapping 5	Configures DNS Host NameMapping for 5th row.	
26	dns host_name mapping 6	Configures DNS Host NameMapping for 6th row.	
27	dns host_name mapping 7	Configures DNS Host NameMapping for 7th row.	
28	dns host_name mapping 8	Configures DNS Host NameMapping for 8th row.	
29	dns host_name mapping 1 host_name	Sets Host Name.	String
30	dns host_name mapping 1 ipaddress	Sets Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
31	dns host_name mapping 2 host_name	Sets Host Name.	String
32	dns host_name mapping 2 ipaddress	Sets Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
33	dns host_name mapping 3 host_name	Sets Host Name.	String
34	dns host_name mapping 3 ipaddress	Sets Host Name.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

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

11.17 net lan ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Saves LAN configuration settings.	
2	exit	Saves LAN configuration settings and exit current mode.	
3	cancel	To revert to the previous LAN configuration settings.	

S.No	Command Name	Description	Type and Description
4	static	Sets system LAN Settings.	
5	static address	Sets 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	Sets system LAN Settings.	
8	dhcp server_enable	Sets dhcpv6 server status.	Boolean choice
9	dhcp mode	DHCPv6 Mode	dhcpv6 modes
10	dhcp domain_name	DHCP server domain name	String, Max 256 characters and no ' or empty space or "
11	dhcp server_preference	Server preference number.	Unsigned integer
12	dhcp dns_type	Dns server type.	dhcpv6 dns server types
13	dhcp primary_dns	Enter 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	Enter secondary dns server.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
15	dhcp rebind_time	Rebind time.	number in range of 0 to 604800

11.18 net lan ipv6 pool configure *<ipv6PoolStartAddr>*

S.No	Command Name	Description	Type and Description
1	*<ipv6PoolStartAddr>*	IPv6 LAN configuration add/edit mode.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
2	save	Saves LAN configuration settings.	
3	exit	Saves LAN configuration settings and exit current mode.	
4	cancel	To revert to the previous LAN configuration settings.	
5	start_address	Sets 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:]

S.No	Command Name	Description	Type and Description
6	end_address	Sets dhcpv6 end IP address.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
7	prefix_value	Prefix length	Unsigned integer

11.19 net lan ipv6 pool delete *<ipv6PoolStartAddr>*

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

11.20 net igmp configure

S.No	Command Name	Description	Type and Description
1	save	Saves igmp settings.	
2	exit	Saves igmp settings and exit current mode.	
3	cancel	To revert to the previous igmp settings settings.	
4	Enable	Specifies the igmp proxy should enable or disable.	Boolean choice
5	UpStreamInterface_WAN1	This command is used to select WAN upstream interface for WAN1.	WAN interface type WAN-DHCP/WAN-PPTP/WAN-L2TP.
6	UpStreamInterface_WAN2	This command is used to select WAN upstream interface for WAN2.	WAN interface type WAN-DHCP/WAN-PPTP/WAN-L2TP.

11.21 net intel_Amt server configure

S.No	Command Name	Description	Type and Description
1	save	Saves InterlAmt server configuration settings.	
2	cancel	To revert to the previous IntelAmt server configuration settings.	
3	exit	Saves IntelAmt server configuration settings and exit current mode.	

S.No	Command Name	Description	Type and Description
4	enable_Intel_Amt	Enables/disables 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 where each part is in the range 0-255.

11.22 net intel_Amt_Reflector configure

S.No	Command Name	Description	Type and Description
1	save	Saves InterlAmt Reflector configuration settings.	
2	cancel	To revert to the previous IntelAmt server configuration settings.	
3	exit	Saves IntelAmt server configuration settings and exit current mode.	
4	enable	Enables intelAmt reflectors on port.	
5	enable Intel_Amt_Reflector	Enables/disables Ports.	Boolean choice
6	enable Intel_Amt_Reflector _destport	Enables intelamt reflectors on different ports.	
7	enable Intel_Amt_Reflector _destport 16992	Enables/disables Ports.	Boolean choice
8	enable Intel_Amt_Reflector _destport 16993	Enables/disables Ports.	Boolean choice
9	enable Intel_Amt_Reflector _destport 16994	Enables/disables Ports.	Boolean choice
10	enable Intel_Amt_Reflector _destport 16995	Enables/disables Ports.	Boolean choice
11	enable Intel_Amt_Reflector _destport 9971	Enables/disables Ports.	Boolean choice
12	Intel_Amt_Reflector _srcport	Sets port number for different ports.	

S.No	Command Name	Description	Type and Description
13	Intel_Amt_Reflector_srcport 16992	Enter source port value for 16992.	Port number
14	Intel_Amt_Reflector_srcport 16993	Enter source port value for 16993.	Port number
15	Intel_Amt_Reflector_srcport 16994	Enter source port value for 16994.	Port number
16	Intel_Amt_Reflector_srcport 16995	Enter source port value for 16995.	Port number
17	Intel_Amt_Reflector_srcport 9971	Enter source port value for 9971.	Port number

11.23 net ip_Aliasing server add

S.No	Command Name	Description	Type and Description
1	save	Saves Ip Alias server configuration settings.	
2	cancel	To revert to the previous Ip Alias server configuration settings.	
3	exit	Saves Ip Aias server configuration settings and exit current mode.	
4	Interface	Selects the Interface for the Ip Aliasing	WAN interface type.
5	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
6	Subnet_Mask	Subnet mask for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.24 net ip_Aliasing server edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Editing Ip Aliasing server configuration.	Unsigned integer
2	save	Saves Ip Alias server configuration settings.	
3	cancel	To revert to the previous Ip Alias server configuration settings.	
4	exit	Saves Ip Aias server configuration settings and exit current mode.	

S.No	Command Name	Description	Type and Description
5	Interface	Select the Interface for the Ip Aliasing	WAN interface type
6	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
7	Subnet_Mask	Subnet mask for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.25 net ip_Aliasing server delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes Ip Aliasing configuration.	Unsigned integer
2	save	Saves Ip Alias server configuration settings.	
3	cancel	To revert to the previous Ip Alias server configuration settings.	
4	exit	Saves Ip Aias server configuration settings and exit current mode.	
5	Interface	Selects the Interface for the Ip Aliasing.	WAN interface type
6	Ip_Address	Ip Address for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	Subnet_Mask	Subnet mask for ip Aliasing.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

11.26 net mode configure

S.No	Command Name	Description	Type and Description
1	save	Saves IP Mode configuration settings.	
2	exit	Saves IP Mode configuration settings and exit current mode.	
3	cancel	To revert to the previous IP Mode configuration settings.	
4	ip_type	Selects IPv4 only or IPv4/IPv6 mode.	Select the ip address type.

11.27 net ipv6_tunnel isatap add

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

11.28 net ipv6_tunnel isatap edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Isatap Tunnel configuration mode.	Unsigned integer
2	save	Saves isatap tunnel configuration settings.	
3	exit	Saves isaptap tunnel configuration settings and exit current mode.	
4	cancel	To revert to the previous isatap tunnel configuration settings.	
5	subnet_prefix	This is the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet.	String

S.No	Command Name	Description	Type and Description
6	end_point_type	This is the endpoint address for the tunnel that starts with this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 network), or a specific LAN IPv4 address.	Select the local end point address type.
7	ipv4_address	The local end point address if not the LAN IPv4 address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

11.29 net ipv6_tunnel isatap delete *<row_id>*

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

11.30 net routing mode configure

S.No	Command Name	Description	Type and Description
1	save	Saves NAT configuration settings.	
2	exit	Saves NAT configuration settings and exit current mode.	
3	cancel	To revert to the previous Basic Security Level configuration settings.	
4	type	Selects NAT or Transparent or Bridge mode.	Routing mode type.
5	bridgeModeSetup	Sets IP Addresses for Bridge and DMZ interfaces in same subnet.	
6	bridgeModeSetup bridge_interfaceIp	Gives bridge Interface ip Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
7	bridgeModeSetup dmz_interfaceIp	Gives DMZ Interface ip Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
8	bridgeModeSetup subnetMask	Gives subnet for the DMZ and Bridge Interfaces.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
9	nat_wanInterface	Selects WAN interfaces for which NAT is to be enabled	Select WAN interface.

11.31 net wan wan1 ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Saves ipv4 wan configuration settings.	
2	cancel	To revert to the previous ipv4 wan configuration settings.	
3	exit	Exits from the current configuration.	
4	isp_connection_type	Selects among the options: STATIC, DHCP Client, PPPoE, PPTP, L2TP, Russian PPTP, Russian L2TP, Japanese Multiple PPPoE, Dual Access PPPoE	ISP Types.
5	dhcpc	If ISP Type selected is DHCPC, this field gives you options to configure DHCPC credentials	
6	dhcpc get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign 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 where each part is in the range 0-255.
9	dhcpc mac_type	Selects the Mac Address Source.	Types of mac address source.
10	dhcpc mac_address	Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where

S.No	Command Name	Description	Type and Description
			each part is in the range 00-FF.
11	dhcpc hostname	Enter the hostname.	String
12	static	If ISP Type selected is STATIC, this field gives you options to configure STATIC credentials.	
13	static ip_address	If your ISP has assigned a fixed (static or permanent) IP address, fill this fields with Static IP address assigned to you. This will identify the router to your ISP.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
14	static subnet_mask	IPv4 Subnet Mask. This is usually provided by the ISP or your network administrator.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
15	static gateway_address	IP address of the ISPâ€™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	Selects 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, Max 64 characters and no ' or empty space or ".
22	pppoe password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or ".
23	pppoe service	Enter the password to authenticate.	String.
24	pppoe authOpt	Enter the Auth Option to authenticate.	PPPOE Authentication Types.

S.No	Command Name	Description	Type and Description
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	Enter valid IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
32	pppoe subnet_mask	Enter valid subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
33	pppoe mac_type	Selects 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.	

S.No	Command Name	Description	Type and Description
36	pptp username	Enter the username to log in.	String, Max 64 characters and no ' or empty space or "
37	pptp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
38	pptp ip_address	If Address Mode is Static, give static ip.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
39	pptp subnet_mask	If Address Mode is Static, give subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
40	pptp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. Otherwise Enter No and give valid static IP address.	Boolean choice
41	pptp mmpe_encryption	Enter the MMPE Encryption.	Boolean choice
42	pptp split_tunnel	Selects the split_tunnel.	Boolean choice
43	pptp gateway	Gateway assigned by the ISP to make a connection with the ISP server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
44	pptp server_address	IP address of the PPTP server (if applicable).	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
45	pptp connectivity_type	Sets ISP Type.	ISP Connectivity Types.
46	pptp idle_time	Sets ISP Type.	Idle timeout value type.
47	pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign a DNS address to the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice
48	pptp primary_dns	Enter valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
49	pptp secondary_dns	Enter valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
50	pptp mac_type	Selects the Mac Address Source.	Types of mac address source.
51	pptp mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
52	russ_pptp	If ISP Type selected is Russian dual access PPTP, this field gives you options to configure credentials.	
53	russ_pptp username	Enter the username to log in.	String, Max 64 characters and no ' or empty space or "
54	russ_pptp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
55	russ_pptp mmpe_encryption	Enter the MMPE Encryption.	Boolean choice
56	russ_pptp split_tunnel	Selects the split_tunnel.	Boolean choice
57	russ_pptp server_address	IP address of the PPTP server (if applicable).	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
58	russ_pptp connectivity_type	Sets the ISP Type.	ISP Connectivity Types.
59	russ_pptp idle_time	Sets the ISP Type.	Idle timeout value type.
60	russ_pptp ip_address	If Address Mode is Static, give static ip.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
61	russ_pptp subnet_mask	If Address Mode is Static, give subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
62	russ_pptp gateway	Gateway assigned by the ISP to make a connection with the ISP server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
63	russ_pptp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. Otherwise Enter No and give valid static IP address.	Boolean choice
64	russ_pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign a DNS address to	Boolean choice

S.No	Command Name	Description	Type and Description
		the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses.	
65	russ_pptp primary_dns	Enter a 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	Enter a alid 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	Selects 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, Max 64 characters and no ' or empty space or "
71	l2tp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
72	l2tp secret	Enter the secret to log in.	String
73	l2tp split_tunnel	Select the split_tunnel.	Boolean choice
74	l2tp gateway	Gateway assigned by the ISP to make a connection with the ISP server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
75	l2tp server_address	IP address of the L2TP server (if applicable).	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
76	l2tp connectivity_type	Sets ISP Type.	ISP Connectivity Types.
77	l2tp idle_time	Sets 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.	Boolean choice

S.No	Command Name	Description	Type and Description
		Otherwise Enter No and give valid static IP address.	
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 a DNS address to the router using L2TP network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice
82	l2tp primary_dns	Valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
83	l2tp secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
84	l2tp mac_type	Selects the Mac Address Source.	Types of mac address source.
85	l2tp mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
86	russ_l2tp	If ISP Type selected is Russian Dual Access L2TP, this field gives you options to configure Russian L2TP credentials.	
87	russ_l2tp username	Enter the username to log in.	String, Max 64 characters and no ' or empty space or "
88	russ_l2tp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
89	russ_l2tp secret	Enter the secret to log in.	String
90	russ_l2tp split_tunnel	Select the split_tunnel.	Boolean choice
91	russ_l2tp server_address	IP address of the L2TP server (if applicable).	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
92	russ_l2tp connectivity_type	Sets ISP Type.	ISP Connectivity Types.
93	russ_l2tp idle_time	Sets ISP Type.	Idle timeout value type.
94	russ_l2tp ip_address	If Address Mode is Static, give static ip.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
95	russ_l2tp gateway	Gateway assigned by the ISP to make a connection with the ISP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
96	russ_l2tp subnet_mask	If Address Mode is Static, give subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
97	russ_l2tp get_ip_from_isp	Enter Yes to get IP dynamically from ISP if you have not been assigned any static IP address. Otherwise Enter No and give valid static IP address	Boolean choice
98	russ_l2tp get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign a DNS address to the router using L2TP network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice
99	russ_l2tp primary_dns	Valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
100	russ_l2tp secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
101	russ_l2tp mac_type	Selects the Mac Address Source.	Types of mac address source.
102	russ_l2tp mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
103	japanese_pppoe	If ISP Type selected is japanese multiple pppoe, this field gives you options to configure credentials.	
104	japanese_pppoe primary_profile	configure the primary pppoe profile	
105	japanese_pppoe primary_profile username	Enter the username to authenticate.	String, Max 64 characters and no ' or empty space or "
106	japanese_pppoe primary_profile password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or "

S.No	Command Name	Description	Type and Description
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 a 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	Configures the secondary pppoe profile.	

S.No	Command Name	Description	Type and Description
118	japanese_pppoe secondary_profile username	Enter the username to authenticate.	String, Max 64 characters and no ' or empty space or "
119	japanese_pppoe secondary_profile password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or "
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 a 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

S.No	Command Name	Description	Type and Description
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, Max 64 characters and no ' or empty space or "
134	dual_pppoe password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or "
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	Boolean choice

S.No	Command Name	Description	Type and Description
		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.	
143	dual_pppoe static_ip	Valid IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
144	dual_pppoe subnet_mask	Valid subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
145	dual_pppoe mac_type	Select the Mac Address Source.	Types of mac address source
146	dual_pppoe mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
147	dual_pppoe get_ip_from_phy	Enter Yes to get ip on physical interface from dhcp server in the internal isp network. Otherwise Enter No and give valid static IP address, subnet mask and gateway.	Boolean choice
148	dual_pppoe static_ip_phy	Valid IP Address of physical interface.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
149	dual_pppoe subnet_mask_phy	Valid subnet mask of physical network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
150	dual_pppoe gateway_phy	Valid gateway of physcial network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
151	dual_pppoe get_dns_from_isp_phy	Enter Yes to get dns dynamically from interal 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

S.No	Command Name	Description	Type and Description
152	dual_pppoe primary_dns_phy	Valid primary DNS Server IP Address of physical network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
153	dual_pppoe secondary_dns_phy	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
154	enable_vlan_tag	Enables vlan on wan1.	Boolean choice
155	vlan_Id	Enter Vlan Id.	Unsigned integer

11.32 net wan wan2 ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Saves ipv4 wan configuration settings.	
2	cancel	To revert to the previous ipv4 wan configuration settings.	
3	exit	Exit from the current configuration.	
4	isp_connection_type	Select among the options: STATIC, DHCP Client, PPPoE, PPTP, L2TP, Russian PPTP, Russian L2TP, Japanese Multiple PPPoE, Dual Access Pppoe, ThreeG	WAN2 ISP Types.
5	dhcpc	If ISP Type selected is DHCPC, this field gives you options to configure DHCPC credentials	
6	dhcpc get_dns_from_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 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.

S.No	Command Name	Description	Type and Description
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 ISPâ€™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, Max 64 characters and no ' or empty space or "
22	pppoe password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or "

S.No	Command Name	Description	Type and Description
23	pppoe service	Enter the password to authenticate.	String
24	pppoe authOpt	Enter the Auth Option to authenticate.	PPPOE Authentication Types.
25	pppoe connectivity_type	Enter the connectivity type.	ISP Connectivity Types.
26	pppoe idletime	Enter the idle time.	Idle timeout value type.
27	pppoe get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign 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	enable_vlan_tag	Enables vlan on wan2.	Boolean choice
31	vlan_Id	Enter Vlan Id.	Unsigned integer
32	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
33	pppoe static_ip	Valid IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
34	pppoe subnet_mask	Valid subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
35	pppoe mac_type	Select the Mac Address Source.	Types of mac address source.
36	pppoe mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where

S.No	Command Name	Description	Type and Description
			each part is in the range 00-FF.
37	pptp	If ISP Type selected is PPTP, this field gives you options to configure PPTP credentials.	
38	pptp username	Enter the username to log in.	String, Max 64 characters and no ' or empty space or "
39	pptp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
40	pptp mmpe_encryption	Enter the MMPE Encryption.	Boolean choice.
41	pptp split_tunnel	Selects the split_tunnel.	Boolean choice.
42	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.
43	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.
44	pptp connectivity_type	Sets the ISP Type.	ISP Connectivity Types.
45	pptp idle_time	Sets the ISP Type.	Idle timeout value type.
46	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.
47	pptp subnet_mask	If Address Mode is Static, give subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
48	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
49	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 a DNS address to the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice

S.No	Command Name	Description	Type and Description
50	pptp primary_dns	Valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
51	pptp secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
52	pptp mac_type	Select the Mac Address Source.	Types of mac address source.
53	pptp mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
54	russ_pptp	If ISP Type selected is Russian dual access PPTP, this field gives you options to configure credentials.	
55	russ_pptp username	Enter the username to log in.	String, Max 64 characters and no ' or empty space or "
56	russ_pptp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
57	russ_pptp mmpe_encryption	Enter the MMPE Encryption.	Boolean choice
58	russ_pptp split_tunnel	Selects the split_tunnel.	Boolean choice
59	russ_pptp server_address	IP address of the PPTP server (if applicable).	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
60	russ_pptp connectivity_type	Sets the ISP Type.	ISP Connectivity Types.
61	russ_pptp idle_time	Sets the ISP Type.	Idle timeout value type.
62	russ_pptp ip_address	If Address Mode is Static, give static ip.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
63	russ_pptp subnet_mask	If Address Mode is Static, give subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
64	russ_pptp gateway	Gateway assigned by the ISP to make a connection with the ISP server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
65	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

S.No	Command Name	Description	Type and Description
66	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 a DNS address to the router using PPTP network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice
67	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.
68	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.
69	russ_pptp mac_type	Selects the Mac Address Source.	Types of mac address source.
70	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.
71	l2tp	If ISP Type selected is L2TP, this field gives you options to configure L2TP credentials.	
72	l2tp username	Enter the username to log in.	String, Max 64 characters and no ' or empty space or "
73	l2tp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
74	l2tp secret	Enter the secret to log in.	String
75	l2tp split_tunnel	Selects the split_tunnel.	Boolean choice
76	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.
77	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.
78	l2tp connectivity_type	Sets the ISP Type.	ISP Connectivity Types.
79	l2tp idle_time	Sets the ISP Type.	Idle timeout value type.
80	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.

S.No	Command Name	Description	Type and Description
81	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.
82	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
83	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 a DNS address to the router using L2TP network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice
84	l2tp primary_dns	Valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
85	l2tp secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
86	l2tp mac_type	Selects the Mac Address Source.	Types of mac address source.
87	l2tp mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
88	russ_l2tp	If ISP Type selected is Russian DualAccessL2TP, this field gives you options to configure L2TP credentials.	
89	russ_l2tp username	Enter the username to log in.	String, Max 64 characters and no ' or empty space or "
90	russ_l2tp password	Enter the password to log in.	String, Max 16 characters and no ' or empty space or "
91	russ_l2tp secret	Enter the secret to log in.	String
92	russ_l2tp split_tunnel	Select the split_tunnel.	Boolean choice

S.No	Command Name	Description	Type and Description
93	russ_l2tp server_address	IP address of the L2TP server (if applicable).	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
94	russ_l2tp connectivity_type	Set ISP Type.	ISP Connectivity Types.
95	russ_l2tp idle_time	Set ISP Type.	Idle timeout value type.
96	russ_l2tp ip_address	If Address Mode is Static, give static ip.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
97	russ_l2tp subnet_mask	If Address Mode is Static, give subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
98	russ_l2tp gateway	Gateway assigned by the ISP to make a connection with the ISP server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
99	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.
100	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 a DNS address to the router using L2TP network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice.
101	russ_l2tp primary_dns	Valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
102	russ_l2tp secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
103	russ_l2tp mac_type	Selects the Mac Address Source.	Types of mac address source.
104	russ_l2tp mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
105	japanese_pppoe	If ISP Type selected is japanese multiple pppoe,	

S.No	Command Name	Description	Type and Description
		this field gives you options to configure credentials.	
106	japanese_pppoe primary_profile	Configure the primary pppoe profile.	
107	japanese_pppoe primary_profile username	Enter the username to authenticate.	String, Max 64 characters and no ' or empty space or "
108	japanese_pppoe primary_profile password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or "
109	japanese_pppoe primary_profile service	Enter the password to authenticate.	String
110	japanese_pppoe primary_profile authOpt	Enter the Auth Option to authenticate.	PPPOE Authentication Types.
111	japanese_pppoe primary_profile connectivity_type	Enter the connectivity type.	ISP Connectivity Types.
112	japanese_pppoe primary_profile idletime	Enter the idle time.	Idle timeout value type.
113	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 a DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice
114	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.
115	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.
116	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.	Boolean choice

S.No	Command Name	Description	Type and Description
		Otherwise Enter No and give valid static IP address.	
117	japanese_pppoe primary_profile static_ip	Valid IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
118	japanese_pppoe primary_profile subnet_mask	Valid subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
119	japanese_pppoe secondary_profile	Configures the secondary pppoe profile.	
120	japanese_pppoe secondary_profile username	Enter the username to authenticate.	String, Max 64 characters and no ' or empty space or "
121	japanese_pppoe secondary_profile password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or "
122	japanese_pppoe secondary_profile service	Enter the password to authenticate.	String
123	japanese_pppoe secondary_profile authOpt	Enter the Auth Option to authenticate.	PPPOE Authentication Types.
124	japanese_pppoe secondary_profile connectivity_type	Enter the connectivity type.	ISP Connectivity Types.
125	japanese_pppoe secondary_profile idletime	Enter the idle time.	Idle timeout value type.
126	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 a DNS address to the router using PPPOE network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice.
127	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.
128	japanese_pppoe secondary_profile secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
129	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
130	japanese_pppoe secondary_profile static_ip	Valid IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
131	japanese_pppoe secondary_profile subnet_mask	Valid subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
132	japanese_pppoe mac_type	Select the Mac Address Source.	Types of mac address source.
133	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.
134	dual_pppoe	If ISP Type selected is Dual PPPoE, this field gives you options to configure Dual Access PPPoE credentials.	
135	dual_pppoe username	Enter the username to authenticate.	String, Max 64 characters and no ' or empty space or "
136	dual_pppoe password	Enter the password to authenticate.	String, Max 16 characters and no ' or empty space or "
137	dual_pppoe service	Enter the service to authenticate.	String
138	dual_pppoe authOpt	Enter the Auth Option to authenticate.	PPPOE Authentication Types.
139	dual_pppoe connectivity_type	Enter the connectivity type.	ISP Connectivity Types.
140	dual_pppoe idletime	Enter the idle time.	Idle timeout value type.
141	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 a DNS address to the router using PPPOE network protocol. Otherwise Enter No and	Boolean choice

S.No	Command Name	Description	Type and Description
		give valid static dns addresses.	
142	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.
143	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.
144	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
145	dual_pppoe static_ip	Valid IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
146	dual_pppoe subnet_mask	Valid subnet mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
147	dual_pppoe mac_type	Select the Mac Address Source.	Types of mac address source.
148	dual_pppoe mac_address	Enter Valid MAC address.	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF.
149	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.
150	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.
151	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.
152	dual_pppoe gateway_phy	Valid gateway of physcial network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
153	dual_pppoe get_dns_from_isp_phy	Enter Yes to get dns dynamically from interal 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.
154	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.
155	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.
156	threeg	If ISP Type selected is THREEG, this field gives you options to configure THREEG credentials.	
157	threeg username	Enter the username to authenticate.	String, Max 256 characters and no ' or empty space or "
158	threeg password	Enter the password to authenticate.	String, Max 256 characters and no ' or empty space or "
159	threeg dial_number	Enter the dail number to connect.	String
160	threeg authMethod	Enter the auth type to connect.	THREEG Authentication Types.
161	threeg apn	Enter the apn to connect.	String
162	threeg connectivity_type	Sets the ISP Type.	ISP Connectivity Types.
163	threeg idle_time	Sets the ISP Type.	Idle timeout value type.
164	threeg get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address. The ISP will automatically assign a DNS address to the router using THREEG network protocol. Otherwise Enter No and give valid static dns addresses.	Boolean choice

S.No	Command Name	Description	Type and Description
165	threeg primary_dns	Valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
166	threeg secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.33 net wan wan3 threeG configure

S.No	Command Name	Description	Type and Description
1	save	Saves wan3 threeG configuration settings.	
2	cancel	To revert to the previous wan3 threeG configuration settings.	
3	exit	Saves wan3 threeG configuration settings and current mode.	
4	Username	Enter the username required to log in to the ISP.	String, Max 256 characters and no ' or empty space or "
5	Password	Enter the password required to login to the ISP.	String, Max 256 characters and no ' or empty space or "
6	Dial_number	Enter the number to dial to the ISP.	String
7	AuthMethod	Selects one of None, PAP or CHAP Authentication Protocols to connect to the ISP.	THREEG Authentication Types.
8	Apn	Enter the APN (Access Point Name) provided by the ISP.	String
9	Reconnect_mode	Selects Always On: The connection is always on OR On Demand: The connection will 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	Boolean choice

S.No	Command Name	Description	Type and Description
		any static IP address. The ISP will automatically assign a DNS address to the router using THREEG network protocol. Otherwise Enter No and give valid static dns addresses.	
12	Primary_dns	Valid primary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
13	Secondary_dns	Valid secondary DNS Server IP Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.34 net wan mode configure

S.No	Command Name	Description	Type and Description
1	save	Saves wan mode configuration settings.	
2	cancel	To revert to the previous ipv4 wan configuration settings.	
3	exit	Saves wan mode configuration settings and current mode.	
4	wan_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	Selects the Fail Over detection method	
8	loadbalancing spillover	Spill Over Configuration Parameters	
9	loadbalancing spillover load_tolerance	Percentage of max bandwidth after which the	Unsigned integer.

S.No	Command Name	Description	Type and Description
		router switches to secondary WAN	
10	loadbalancing spillover max_bandwidth	Sets the maximum bandwidth tolerable by the Primary WAN. If the bandwidth goes below the load tolerance value of configured Max Bandwidth, the router switches to secondary WAN.	Unsigned integer.
11	loadbalancing spillover max_bandwidth_unit	Sets the maximum bandwidth unit tolerable by the Primary WAN. If the bandwidth goes below the load tolerance value of configured Max Bandwidth, the router switches to secondary WAN.	Types of max bandwidth unit.
12	loadbalancing failover_method type	Select the Fail Over detection method	Types of Faillover Detection methods.
13	loadbalancing failover_method dns		
14	loadbalancing failover_method dns ipaddr_wan1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
15	loadbalancing failover_method dns ipaddr_wan2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
16	loadbalancing failover_method dns ipaddr_wan3		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
17	loadbalancing failover_method ping		
18	loadbalancing failover_method ping ipaddr_wan1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
19	loadbalancing failover_method ping ipaddr_wan2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
20	loadbalancing failover_method ping ipaddr_wan3		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
21	loadbalancing failover_method retry_interval		Idle timeout value type.
22	loadbalancing failover_method retry_attempts		Number in range of 2 to 999.
23	rollover	Wan Mode in Auto Rollover	
24	rollover wan_port	Selects the Auto rollover WAN port	WAN interface type
25	rollover wan_port_Sec	Select the Auto rollover WAN port	WAN interface type
26	rollover failover_method	Selects the Fail Over detection method	
27	rollover failover_method type	Selects the Fail Over detection method	Types of Faillover Detection methods.
28	rollover failover_method dns		
29	rollover failover_method dns ipaddr_wan1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
30	rollover failover_method dns ipaddr_wan2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
31	rollover failover_method dns ipaddr_wan3		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
32	rollover failover_method ping		
33	rollover failover_method ping ipaddr_wan1		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
34	rollover failover_method ping ipaddr_wan2		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
35	rollover failover_method ping ipaddr_wan3		IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
36	rollover failover_method retry_interval		Idle timeout value type.
37	rollover failover_method retry_attempts		Number in range of 2 to 999.

S.No	Command Name	Description	Type and Description
38	singleport		
39	singleport wan_port		WAN interface type.

11.35 net wan port_setup configure

S.No	Command Name	Description	Type and Description
1	save	Saves WAN port settings.	
2	exit	Saves WAN port settings and exit current mode.	
3	cancel	To revert to the previous WAN port settings settings.	
4	respond_ping	Disables or Enables ping on WAN side	Boolean choice.
5	wan1	WAN1 port settings	
6	wan1 mtu_type	Enter MTU type.	Mtu type.
7	wan1 mtu_size	Enter MTU size for WAN1.	Mtu size.
8	wan1 port_speed	Enter the type of port speed for WAN1.	Port Speed types.
9	wan2	WAN2 port settings.	
10	wan2 mtu_type	Enter MTU type.	Mtu type.
11	wan2 mtu_size	Enter MTU size for WAN2.	Mtu size.
12	wan2 port_speed	Enter the type of port speed for WAN2.	Port Speed types.

11.36 net wan vlan_setup configure

S.No	Command Name	Description	Type and Description
1	save	Saves WAN port vlan settings.	
2	exit	Saves WAN vlan settings and exit current mode.	
3	cancel	To revert to the previous WAN vlan settings settings.	
4	trunk_mode	Disables or Enables Trunk Mode Vlan.	Boolean choice
5	force_recegotiation	Disables or Enables Force renegotiation on WAN.	Boolean choice

11.37 net wan vlan_setup vlanId_Add

S.No	Command Name	Description	Type and Description
1	save	Saves WAN port vlan Add settings.	

S.No	Command Name	Description	Type and Description
2	exit	Saves WAN vlan Add settings and exit current mode.	
3	cancel	To revert to the previous WAN vlan settings settings.	
4	vlan_Id	Enter Vlan Id.	Unsigned integer

11.38 net wan vlan_setup vlanId_Delete

S.No	Command Name	Description	Type and Description
1	save	Saves WAN port vlan Delete settings.	
2	exit	Saves WAN vlan Delete settings and exit current mode.	
3	cancel	To revert to the previous WAN vlan settings settings.	
4	vlan_Id	Enter Vlan Id.	Unsigned integer

11.39 net wan configurable_port configure

S.No	Command Name	Description	Type and Description
1	save	Saves Configurable WAN settings.	
2	exit	Saves configurable WAN settings and exit current mode.	
3	cancel	To revert to the previous Configurable WAN settings settings.	
4	port_name	Selects the configurable port type.	WAN interface type

11.40 net wan wan1 ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Saves ipv6 wan1 configuration settings.	
2	cancel	To revert to the previous ipv6 wan configuration settings.	

S.No	Command Name	Description	Type and Description
3	exit	Saves ipv6 wan1 configuration settings and current mode.	
4	isp_type	Sets the ISP Type.	ISP Types.
5	dhcpc	Sets the DHCPC Configurations.	
6	dhcpc stateless_mode_enable	Sets the Stateless Mode.	Stateless mode configuration.
7	dhcpc prefix_delegation_enable	Enables prefix delegation.	Boolean choice
8	static	Sets ipv6 address.	
9	static ip_address	Sets 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	Sets the prefix length.	Unsigned integer
11	static gateway_address	Sets the 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	Sets the 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	Sets the 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:]

S.No	Command Name	Description	Type and Description
20	pppoe secondary_dns	Valid secondary DNS Server IP Address.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]

11.41 net wan wan2 ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Saves ipv6 wan2 configuration settings.	
2	cancel	To revert to the previous ipv6 wan2 configuration settings.	
3	exit	Saves ipv6 wan2 configuration settings and current mode.	
4	isp_type	Sets the ISP Type.	ISP Types.
5	dhcpc	Sets the DHCPC Configurations.	
6	dhcpc stateless_mode_enable	Sets the Stateless Mode.	Stateless mode configuration.
7	dhcpc prefix_delegation_enable	Enables prefix delegation.	Boolean choice
8	static	Sets the ipv6 address.	
9	static ip_address	Sets the 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	Sets the prefix length.	Unsigned integer
11	static gateway_address	Sets the 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	Sets the 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	Sets the ipv6 secondary dns address.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
14	pppoe	PPPoE over ipv6 configuration parameters.	

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

11.42 net routing ospfv2 configure *<interface>*

S.No	Command Name	Description	Type and Description
1	*<interface>*	Ospfv2 configuration mode.	OSPF Interfaces type
2	save	Saves OSPFv2 configuration settings.	
3	exit	Saves OSPFv2 configuration settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
5	enable	Enables/Disables OSPFv2 for a particular interface.	Boolean choice
6	area	Gives the area to which the interface belongs.	Unsigned integer
7	priority	Helps to determine the OSPFv2 designated router for a network. The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0, makes the router ineligible to be come Designated Router. The default value is 1.	Unsigned integer

S.No	Command Name	Description	Type and Description
8	hello_interval	The number of seconds for HelloInterval timervalue. 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	Gives the authentication type used for OSPFv2. If Authentication type is **none,** the interface does not authenticate ospf packets. If Authentication Type is **Simple,** ospf packets are authenticated using simple text key. If Authentication Type is **MD5,** 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	Gives the MD5 Key id.	Unsigned integer
14	md5_auth_key	Gives the MD5 text key.	String

11.43 net routing ospfv3 configure *<interface>*

S.No	Command Name	Description	Type and Description
1	*<interface>*	Ospfv3 configuration mode.	OSPF Interfaces type
2	save	Saves OSPFv3 configuration settings.	
3	exit	Saves OSPFv3 configuration settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
5	enable	Enables/Disables 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 beco me 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 defaul t value is 40 seconds.	Unsigned integer

S.No	Command Name	Description	Type and Description
9	cost	The cost of sending a packet on an OSPFv3 interface.	Unsigned integer

11.44 16.44 net routing protocol_binding add

S.No	Command Name	Description	Type and Description
1	save	Saves Protocol-Binding rules configuration settings.	
2	exit	Saves Protocol Binding rules configuration settings and exit current mode.	
3	cancel	To revert to the previous configuration settings.	
4	Service	Available Service.	service type
5	Local_Gateway	Local gateway type.	WAN interface type
6	Source_Network	Source network type.	Firewall rule address type.
7	Destination_Network	Destination network type.	Firewall rule address type.
8	source_address_start	Starting IP of the Source Network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
9	source_address_end	Ending IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
10	destination_address_start	Sets the start IP of the Destination user range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
11	destination_address_end	Sets the last IP of the Destiation use range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.45 net routing protocol_binding edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Protocol_binding rules configuration mode.	Unsigned integer
2	save	Saves Protocol-Binding rules configuration settings.	
3	exit	Saves Protocol Binding rules configuration settings and exit current mode.	

S.No	Command Name	Description	Type and Description
4	cancel	To revert to the previous configuration settings.	
5	Service	Available Service.	service type
6	Local_Gateway	Local gateway type.	WAN interface type
7	Source_Network	Source network type.	firewall rule address type
8	Destination_Network	Destination network type.	firewall rule address type
9	source_address_start	Starting IP of the Source Network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	source_address_end	Ending IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	destination_address_start	Start IP of the Destination user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	destination_address_end	Ending IP of the Destiation user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

11.46 net routing protocol_binding enable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Protocol_binding rules configuration mode.	Unsigned integer
2	save	Saves Protocol-Binding rules configuration settings.	
3	exit	Saves Protocol Binding rules configuration settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
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.

S.No	Command Name	Description	Type and Description
11	destination_address_start	First IP of the Destination user address range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
12	destination_address_end	Last IP of the Destiation user address range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.47 net routing protocol_binding disable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Protocol_binding rules configuration mode.	Unsigned integer.
2	save	Saves Protocol-Binding rules configuration settings.	
3	exit	Saves Protocol Binding rules configuration settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
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	First IP of the Source Network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
10	source_address_end	Last IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
11	destination_address_start	First IP of the Destination user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
12	destination_address_end	Last IP of the Destiation user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.48 net routing protocol_binding delete *<row_id>*

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

S.No	Command Name	Description	Type and Description
2	save	Saves Protocol-Binding rules configuration settings.	
3	exit	Save Protocol Binding rules configuration settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
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	First IP address of the Source Network.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
10	source_address_end	Last IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
11	destination_address_start	First IP of the Destination user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
12	destination_address_end	Last IP of the Destiation user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

11.49 net radvd configure

S.No	Command Name	Description	Type and Description
1	save	Saves radvd configuration settings.	
2	exit	Saves radvd configuration settings and exit current mode.	
3	cancel	To revert to the previous radvd configuration settings.	
4	enable	Enables the RADVD process here to allow stateless auto configuration of the IPv6 LAN network.	Boolean choice
5	mode	Selects N to send router advertisements (RA's) to all interfaces, else Y.	Radvd advertizement mode type.
6	interval	The time in seconds between sending	PPPOE idle timeout Type.

S.No	Command Name	Description	Type and Description
		unsolicited multicast RA's. The default is 30 seconds.	
7	flags	RA Flags	
8	flags managed_enable	Selects 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	Selects low/medium/high for the preference associated with this router's RADVD process.	Radvd preference type.
11	mtu	This is used in RAâ€™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.

11.50 net radvd pool add

S.No	Command Name	Description	Type and Description
1	save	Saves radvd Pool configuration settings.	
2	exit	Saves radvd Pool configuration settings and exit current mode.	
3	cancel	To revert to the previous radvd Pool configuration settings.	
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	Unsigned integer.

S.No	Command Name	Description	Type and Description
		interface on which the advertisements are sent.	
6	prefix_address	It specifies the IPv6 network address.	String
7	prefix_length	The prefix length variable is a decimal value that indicates the number of contiguous, higher order bits of the address that make up the network portion of the address.	Unsigned integer
8	prefix_life_time	The length of time over which the requesting router is allowed to use the prefix.	Unsigned integer

11.51 net radvd pool edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Radvd Pool configuration mode.	Unsigned integer.
2	save	Saves radvd Pool configuration settings.	
3	exit	Saves radvd Pool configuration settings and exit current mode.	
4	cancel	To revert to the previous radvd Pool configuration settings.	
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	Unsigned integer.

S.No	Command Name	Description	Type and Description
		make up the network portion of the address.	
9	prefix_life_time	The length of time over which the requesting router is allowed to use the prefix.	Unsigned integer

11.52 net radvd pool delete *<row_id>*

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

11.53 net routing dynamic configure

S.No	Command Name	Description	Type and Description
1	save	Saves dynamic route settings.	
2	exit	Saves dynamic routes settings and exit current mode.	
3	cancel	To revert to the previous rip configuration settings.	
4	direction	Rip direction can be None, In only, Out only, Both.	Rip direction.
5	version	Rip version.	Rip version.
6	authentication_enable	Enables/Disables Authentication for RIP-2B/2M.	Boolean choice.
7	first_key	First MD5 key.	
8	first_key id_number	First MD5 Key Id.	Unsigned integer
9	first_key authentication_id	First MD5 Authentication Key.	String
10	first_key valid_from	First MD5 Key Not Valid Before entered date.	
11	first_key valid_from month	Month in which md5 authentication key validity starts.	Month in the format MM(01-12)
12	first_key valid_from day	Day in which md5 authentication key validity starts.	Day in the format DD(01-31)
13	first_key valid_from year	Year in which md5 authentication key validity starts.	Year

S.No	Command Name	Description	Type and Description
14	first_key valid_from hour	Hour in which md5 authentication key validity starts.	HH(00-23) using 24 hour clock
15	first_key valid_from minute	Minute in which md5 authentication key validity starts.	Minute in the format MM(00-59.)
16	first_key valid_from second	Second in which md5 authentication key validity starts.	Second in the format SS(00-59).
17	first_key valid_to	First MD5 Key is Not Valid After entered date.	
18	first_key valid_to month	Month in which md5 authentication key validity ends.	Month in the format MM(01-12)
19	first_key valid_to day	Day in which md5 authentication key validity ends.	Day in the format DD(01-31)
20	first_key valid_to year	Year in which md5 authentication key validity ends.	Year
21	first_key valid_to hour	Hour in which md5 authentication key validity ends.	HH(00-23) using 24 hour clock
22	first_key valid_to minute	Minute in which md5 authentication key validity ends.	Minute in the format MM(00-59).
23	first_key valid_to second	Second in which md5 authentication key validity ends.	Second in the format SS(00-59)
24	second_key	Second MD5 Key Parameters.	
25	second_key id_number	Second MD5 Key Id.	Unsigned integer
26	second_key authentication_id	Second MD5 Authentication Key.	String
27	second_key valid_from	Second MD5 Key Not Valid Before Entered date.	
28	second_key valid_to	Second MD5 Key Not Valid After entered date.	
29	second_key valid_from month	Month in which md5 authentication key validity starts.	Month in the format MM(01-12)
30	second_key valid_from day	Day in which md5 authentication key validity starts.	Day in the format DD(01-31)

S.No	Command Name	Description	Type and Description
31	second_key valid_from year	Year in which md5 authentication key validity starts.	Year
32	second_key valid_from hour	Hour in which md5 authentication key validity starts.	HH(00-23) using 24 hour clock
33	second_key valid_from minute	Minute in which md5 authentication key validity starts.	Minute in the format MM(00-59).
34	second_key valid_from second	Second in which md5 authentication key validity starts.	Second in the format SS(00-59)
35	second_key valid_to month	Month in which md5 authentication key validity ends.	Month in the format MM(01-12)
36	second_key valid_to day	Day in which md5 authentication key validity ends.	Day in the format DD(01-31)
37	second_key valid_to year	Year in which md5 authentication key validity ends.	Year
38	second_key valid_to hour	Hour in which md5 authentication key validity ends.	HH(00-23) using 24 hour clock
39	second_key valid_to minute	Minute in which md5 authentication key validity ends.	Minute in the format MM (00-59).
40	second_key valid_to second	Second in which md5 authentication key validity ends.	Second in the format SS(00-59)

11.54 net routing static ipv4 configure *<name>*

S.No	Command Name	Description	Type and Description
1	*<name>*	Adds new static routes.	String
2	save	Saves static route settings.	
3	exit	Saves static routes settings and exit current mode.	
4	cancel	To revert to the previous route configuration settings.	
5	destination_address	Sets the destination IP.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
6	subnet_mask	Sets the subnet for this rule.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	gateway_address	Sets the gateway IP.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	interface	Sets the interface for which the rule applies.	Use show net routing static interface_list to see list of interface
9	metric	Sets the metric for this route.	Unsigned integer
10	private_flag	Defines whether the route can be shared with other gateways when RIP is enabled.	Boolean choice
11	active_flag	Defines whether it's an active route.	Boolean choice

11.55 net routing static ipv6 configure *<name>*

S.No	Command Name	Description	Type and Description
1	*<name>*	Adds new IPV6 static routes.	String
2	save	Saves IPV6 static route settings.	
3	exit	Saves IPV6 static routes settings and exit current mode.	
4	cancel	To revert to the previous IPV6 route configuration settings.	
5	destination_address	Sets 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	Sets the prefix length for this rule.	Unsigned integer
7	gateway_address	Sets 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	Sets the interface for which the rule applies.	select the ipv6 interface type

S.No	Command Name	Description	Type and Description
9	metric	Sets the metric for this route.	Unsigned integer
10	active_flag	Defines whether its an active IPV6 route	Boolean choice

11.56 net routing static ipv4 delete *<name>*

S.No	Command Name	Description	Type and Description
1	*<name>*	Deletes a specific IPv4 route.	String

11.57 net routing static ipv6 delete *<name>*

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

11.58 net tahi add-default-route *<ip_address>*

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

11.59 net tahi add-route *<ip_address> <gw>*

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

11.60 net tahi del-route *<ip_address> <gw>*

S.No	Command Name	Description	Type and Description
1	*<ip_address> <gw>*	Adds ipv6 route on lan interface.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is

S.No	Command Name	Description	Type and Description
			in the range [0-9A-Fa-f:] IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]

11.61 net tahi ipv6-Alias-Add(LAN) *<ip6_address>*

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

11.62 net tahi ipv6-Alias-Del(LAN) *<ip6_address>*

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

11.63 net tahi ipv6-Alias-Add(WAN) *<ip6_address>*

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

11.64 net tahi ipv6-Alias-Del(WAN) *<ip6_address>*

S.No	Command Name	Description	Type and Description
1	*<ip6_address>*	Deletes an ipv6 address from WAN interface.	IP address abcd:abcd:abcd:abcd:abcd:abc

S.No	Command Name	Description	Type and Description
			d:abcd:abcd where each part is in the range [0-9A-Fa-f:]

11.65 net tahi reachable-time *<time>*

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

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

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

11.67 net tahi mping6 *<mip>*

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

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

S.No	Command Name	Description	Type and Description
1	*<bip> <psize>*	Ping6.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:] number in range of 1 to 1500

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

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

11.70 net tahi interface-down *<interface>*

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

11.71 net tahi interface-up *<interface>*

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

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

S.No	Command Name	Description	Type and Description
1	*<fileName> <ipAddr>*	Starts RA with configuration file obtained through tftp.	String IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

11.73 net tahi RA-Start

S.No	Command Name	Description	Type and Description
1	save	Saves RA configuration settings.	
2	exit	Starts RA, and exits current mode.	
3	cancel	To revert to the previous RA configuration settings.	
4	Interface	Interface on which RA should be sent.	Interfaces type
5	AdvSendAdvert	Sets AdvSendAdvert value.	Boolean choice
6	MaxRtrAdvInterval	Sets MaxRtrAdvInterval value.	MaxRtrAdvInterval range
7	MinRtrAdvInterval	Sets MinRtrAdvInterval value.	MinRtrAdvInterval range
8	AdvCurHopLimit	Sets AdvCurHopLimit value.	AdvCurHopLimit range
9	AdvManagedFlag	Sets AdvManagedFlag value.	Boolean choice

S.No	Command Name	Description	Type and Description
10	AdvOtherConfigFlag	Sets AdvOtherConfigFlag value.	Boolean choice
11	AdvDefaultLifetime	Sets AdvDefaultLifetime value.	AdvDefaultLifetime range
12	AdvReachableTime	Sets AdvReachableTime value.	AdvReachableTime range
13	AdvRetransTimer	Sets AdvRetransTimer value.	AdvRetransTimer range
14	AdvLinkMTU	Sets AdvLinkMTU value.	AdvLinkMTU range
15	prefix	Prefix to be advertised.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
16	prefixLength	Sets prefix length value.	IPv6 Prefix length
17	AdvOnLink	Sets AdvOnLink value.	Boolean choice
18	AdvAutonomous	Sets AdvAutonomous value.	Boolean choice
19	AdvValidLifetime	Sets AdvValidLifetime value.	AdvValidLifetime range
20	AdvPreferredLifetime	Sets AdvPreferredLifetime value.	AdvPreferredLifetime range

11.74 net ipv6_tunnel teredo configure

S.No	Command Name	Description	Type and Description
1	save	Saves teredo Tunnel configuration settings.	
2	exit	Saves teredo Tunnel configurationsettings and exit current mode.	
3	cancel	To revert to the previous teredoTunnel configuration settings.	
4	teredo_tunneling_enable	Enables/disables teredo tunneling which will allow traffic from a LAN IPv6 network to be tunneled through a WAN IPv4 network to reach an IPV6 network.	Boolean choice
5	primary_teredo_server	Primary teredo server.	String
6	secondary_teredo_server	Secondary teredo server.	String

11.75 net upnp configure

S.No	Command Name	Description	Type and Description
1	save	Saves upnp configuration settings.	
2	cancel	To revert to the previous upnp configuration settings.	
3	exit	Saves upnp configuration settings and current mode.	
4	enable	Enables/Disables UPNP.	Boolean choice
5	Interface	Selects the interface from LAN/VLAN.	String
6	advertisement	Sets upnp advertisement parameters.	
7	advertisement period	Sets Advertisement Period (in seconds).	UPnP Advertisement Period Type.
8	advertisement time_to_live	Sets Advertisement Time To Live (in seconds).	UPnP Advertisement Time To Live Type.
9	avail_vlan	Displays available vlan.	

11.76 net port-vlan lan_edit *<portnamew>*

S.No	Command Name	Description	Type and Description
1	*<portnamew>*	Vlan port name range 1-4.	port ID
2	save	Saves vlan configuration settings.	
3	exit	Saves vlan settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
5	mode	Port Vlan mode.	Captive Portal Profile ID
6	pvid	Port Vlan ID.	vlan id possible values

11.77 net port-vlan wlan_edit *<ssidName>*

S.No	Command Name	Description	Type and Description
1	*<ssidName>*	SSID to be edited.Use command 'show net wireless_vlan status 'to dislay all SSID's Name	String
2	save	Saves vlan configuration settings.	
3	exit	Saves vlan settings and exit current mode.	

S.No	Command Name	Description	Type and Description
4	cancel	To revert to the previous configuration settings.	
5	mode	Port Vlan mode.	Captive Portal Profile ID
6	pvid	Port Vlan ID	vlan id possible values

11.78 net vlan-membership lan_edit *<portw>*

S.No	Command Name	Description	Type and Description
1	*<portw>*	Net vlan membership for the vlan and Wlan port.	port ID
2	save	Saves Vlan Membership configuration settings.	
3	cancel	To revert to the previous vlan membership configuration settings.	
4	exit	Saves vlan membership configuration. Settings and exit current mode.	
5	membership	Vlan membership.Give comma seperated VLAN ID values.	
6	membership add	Vlan membership.Give comma seperated VLAN ID values.	String
7	membership remove	Vlan membership.Give comma seperated VLAN ID values.	String

11.79 net vlan-membership wlan_edit *<ssidName>*

S.No	Command Name	Description	Type and Description
1	*<ssidName>*	SSID to be edited.Use command 'show net wireless_vlan status 'to dislay all SSID's Name	String
2	save	Saves Vlan Membership configuration settings.	
3	cancel	To revert to the previous vlan membership configuration settings.	

S.No	Command Name	Description	Type and Description
4	exit	Saves vlan membership configuration settings and exit current mode.	
5	membership	Vlan membership.Give comma seperated VLAN ID values.	
6	membership add	Vlan membership.Give comma seperated VLAN ID values.	String
7	membership remove	Vlan membership.Give comma seperated VLAN ID values.	String

11.80 net multiVlan subnet edit *<vlanID>*

S.No	Command Name	Description	Type and Description
1	*<vlanID>*	Multivlan server edit mode	vlan id possible values
2	save	Saves Multi Vlan server configuration settings.	
3	cancel	To revert to the previous Multi Vlan server configuration settings.	
4	exit	Saves Multivlan server configuration settings and exit current mode.	
5	ip-address	IP of given MultiVlan subnetVlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	subnet-mask	Adds subnet mask for Multivlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	dhcp-mode	Selects the DHCP Mode.	dhcpv4 modes
8	domain-name	Domain name for vlan.	String, Max 256 characters and no ' or empty space or "
9	start-ip	Starting ip address of the dhcp mode.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
10	end-ip	Ending ip of the Valn.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	primary-dns	Primary dns for the vlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

S.No	Command Name	Description	Type and Description
12	secondary-dns	Secondary dns for the vlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	default_gw	Sets default gateway.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	lease-time	Lease time for the vlan.	number in range of 1 to 24
15	relay-gateway	Relay gateway for the vlan.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
16	enable-dns-proxy	Relay gateway for the vlan.	Boolean choice

11.81 net vlan config add *<vlan_id>*

S.No	Command Name	Description	Type and Description
1	*<vlan_id>*	Adds a vlan.	vlan id possible values
2	save	Saves vlan configuration settings.	
3	exit	Saves vlan settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
5	vlan-name	Name for vlan.	String
6	inter-vlan-routing	Enables/Disables interVlan Routing.	Boolean choice
7	showCP-profiles	Available captive portal profiles.	
8	captive-portal-enable	Enables captive portal.	Boolean choice
9	captive-portal-user	AccessType is Permanent User.	
10	captive-portal-user auth-mode	Authentication-server for user.	Authentication Type for Captive Portal user
11	captive-portal-user auth-type	Authentication-type for user.	Radius Authentication type
12	captive-portal-user CP-profile	Captive portal profile for user.	Captive Portal Profile ID
13	captive-portal-user Redirect-Type	Captive portal profile for user.	network redirect mode

11.82 net vlan config edit *<vlan_Id>*

S.No	Command Name	Description	Type and Description
1	*<vlan_Id>*	Edits a configured vlan.	vlan id possible values
2	save	Saves vlan configuration settings.	
3	exit	Saves vlan settings and exit current mode.	
4	cancel	To revert to the previous configuration settings.	
5	vlan-name	Name for vlan.	String
6	inter-vlan-routing	Enables/Disables interVlan Routing.	Boolean choice
7	showCP-profiles	Available captive portal profiles	
8	captive-portal-enable	Enables captive portal	Boolean choice
9	captive-portal-user	AccessType is Permanent User.	
10	captive-portal-user auth-mode	Authentication-server for user.	Authentication Type for Captive Portal user.
11	captive-portal-user auth-type	Authentication-type for user.	Radius Authentication type.
12	captive-portal-user CP-profile	Captive portal profile for user.	Captive Portal Profile ID.
13	captive-portal-user Redirect-Type	Captive portal profile for user.	Network redirect mode.

11.83 net vlan config delete *<VlanId>*

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

11.84 net dmz configure

S.No	Command Name	Description	Type and Description
1	save	Saves van configuration mode.	
2	cancel	To revert to the previous dmz configuration settings.	
3	exit	Saves dmz configuration settings and current mode.	
4	enable_dmz	Enables/Disables DMZ.	Enables/disables dmz.

S.No	Command Name	Description	Type and Description
5	ip_address	Static IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
6	subnet_mask	Subnet Mask.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
7	dhcp_mode	Sets the DHCP mode.	dhcpv4 modes
8	domain_name	DHCP Domain Name.	String, Max 256 characters and no ' or empty space or "
9	starting_ip_address	DHCP Starting IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
10	ending_ip_address	DHCP ending IP address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
11	primary_dns_server	Primary DNS address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
12	secondary_dns_server	Secondary DNS server address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
13	default_gw	Setup default gateway.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
14	wins_server	Sets the DHCP WINS server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
15	lease_time	Sets the DHCP lease time.	Unsigned integer
16	relay_gateway	Sets the DHCP Relay gateway server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
17	dns_proxy_enable	Sets the DNS proxy Enable/Disable.	Boolean choice
18	enable_ldap	Enables/Disables LDAP Server Info.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

Chapter 12. Configuration commands under branch SECURITY

12.1 security advanced_network attack_checks configure

S.No	Command Name	Description	Type and Description
1	save	Saves Security Checks configuration settings.	
2	exit	Saves Security Checks configuration settings and exit current mode.	
3	cancel	To revert to the previous Security Checks configuration settings.	
4	enable_stealth_mode	Enables or Disables Stealth Mode.	Boolean choice
5	block_tcp_flood	Enables or DisablesTCP Flood on WAN port.	Boolean choice
6	block_udp_flood	Enables or DisablesUDP Flood on LAN port.	Boolean choice
7	udp_connection_limit	Connection limit of UDP on LAN port.	Range of simultaneous active UDP connections to be accepted from a single computer on the LAN.
8	allow_lan_icmp	Enables or Disables ICMP Notification on LAN port.	Boolean choice
9	block_spoofed_packets	Allows/Blocks spoofed packets.	Boolean choice
10	Tcp_Filter_Check	Allows/Blocks Tcp Filter Check.	Boolean choice
11	block_icmp_notification	Enables or Disables ICMP notifications on Internet Ports.	Boolean choice
12	block_fragmented_packets	Enables or Disables Fragmented Packets on Internet Ports.	Boolean choice
13	block_multicast_packets	Enables or Disables Multicast packets on Internet Ports.	Boolean choice
14	synflood_dectect_rate	Configures the Syn flood Detect Rate.	Range of packets sent per second in dos attack types.

S.No	Command Name	Description	Type and Description
15	block_spoofed_tcp_rst	Enables or Disables blocking of spoofed tcp RST packets.	Boolean choice
16	block_ftp_bounce_attack	Enables or Disables blocking of FTP Bounce Attack packets.	Boolean choice
17	echostorm_flood_rate	Configures the Echo Storm Flood Rate	Range of packets sent per second in dos attack types.
18	icmp_flood_rate	Configures the ICMP flood Rate	Range of packets sent per second in dos attack types.

12.2 security advanced_network ips setup

S.No	Command Name	Description	Type and Description
1	save	Saves ips configuration settings.	
2	exit	Saves ips configuration settings and exit current mode.	
3	cancel	To revert to the previous ips configuration settings.	
4	enable_intrusion_prevention	Enables or Disables Intrusion Prevention.	Boolean choice
5	enable_intrusion_detection	Enables or Disables Intrusion Detection.	Boolean choice
6	ips_check_active	Enables or Disables IPS checks.	
7	ips_check_active lan-wan	Enables or Disables ips checks active between LAN and WAN.	Boolean choice
8	ips_check_active dmz-wan	Enables or Disables ips checks active between DMZ and WAN.	Boolean choice

12.3 security application_rules add

S.No	Command Name	Description	Type and Description
1	save	Saves application rules configuration settings.	
2	exit	Saves application rules rules configuration settings, and exits current mode.	

S.No	Command Name	Description	Type and Description
3	cancel	To revert to the previous application rules configuration settings.	
4	name	Name of the rule.	String
5	enable_rule	Specifies whether to Enable or Disable the rule.	Boolean choice
6	protocol	Specifies whether the port uses the TCP or UDP protocol.	Type of protocol to be selected for a application rules.
7	interface	Displays interface name on which port triggering rule is configured.	interface type
8	outgoing_start_port	Start port number of the outgoing traffic.	Port number
9	outgoing_end_port	Last port of the outgoing traffic.	Port number
10	incoming_start_port	Start port number of the incoming traffic.	Port number
11	incoming_end_port	Last port number of the incoming traffic.	Port number

12.4 security application_rules edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Application rules configuration mode to edit the selected rule.	Unsigned integer
2	save	Saves application rules configuration settings.	
3	exit	Saves application rules rules configuration settings, and exits current mode.	
4	cancel	To revert to the previous application rules configuration settings.	
5	name	Name of the rule.	String
6	enable_rule	Specifies whether to Enable or Disable the rule.	Boolean choice
7	protocol	Specifies whether the port uses the TCP or UDP protocol.	Type of protocol to be selected for an application rules.
8	interface	Displays interface name on which port triggering rule is configured.	Interface type.

S.No	Command Name	Description	Type and Description
9	outgoing_start_port	First port number of the outgoing traffic.	Port number
10	outgoing_end_port	Last port of the outgoing traffic.	Port number
11	incoming_start_port	Start port number of the incoming traffic.	Port number
12	incoming_end_port	End port number of the incoming traffic.	Port number

12.5 security application_rules delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes the selected rule or rules.	Unsigned integer

12.6 security firewall custom_service add

S.No	Command Name	Description	Type and Description
1	save	Saves custom services configuration settings.	
2	exit	Saves custom services configuration settings and exit current mode.	
3	cancel	To revert to the previous custom services configuration settings.	
4	name	Name of the service for which a rule is to be added.	String
5	protocol	Protocol	Type of protocol to be selected for a custom service.
6	type	Port type can be Port Range/Multiple Ports. The layer 3 Protocol that the service uses. Can be TCP, UDP, BOTH, ICMP or ICMPv6	Type to be selected for a custom service.
7	start_port	Port number of the Destination user.	Port number
8	icmp_type	Port number of the Destination user.	number in range of 0-40(icmp) or 1-255(icmpv6)
9	finish_port	Port of the Destiation user.	Port number
10	multiple_port	Muliple Port of the Destiation user.Seperate Ports by Comma.	String

12.7 security firewall custom_service edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Opens the Custom Services Configuration page, to edit the selected custom Service.	Unsigned integer
2	save	Saves custom services configuration settings.	
3	exit	Saves custom services configuration settings and exit current mode.	
4	cancel	To revert to the previous custom services configuration settings.	
5	name	Name of the service for which a rule is to be added.	String
6	protocol	Protocol.	Type of protocol to be selected for a custom service.
7	type	Port type can be Port Range/Multiple Ports.	Type to be selected for a custom service.
8	start_port	Port number of the Destination user.	Port number
9	icmp_type	Port number of the Destination user.	Number in range of 0-40(icmp) or 1-255(icmpv6).
10	finish_port	Port of the Destiation user.	Port number
11	multiple_port	Muliple Port of the Destiation user. Seperate Ports by Comma.	String

12.8 security firewall custom_service delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes the selected custom service or custom services.	Unsigned integer.

12.9 security firewall ipv4 configure

S.No	Command Name	Description	Type and Description
1	save	Saves Firewall IPV4 rules configuration settings.	
2	exit	Saves Firewall IPV4 rules configuration settings and exit current mode.	
3	cancel	To revert to the previous IPV4 rules configuration settings.	
4	from_zone	Sets from Zone security type.	firewall rule type
5	from_zone_vlan	Sets From Zone VLAN using corresponding VLAN name.	String
6	to_zone	Sets to Zone security type	Firewall rule type.
7	to_zone_vlan	Sets To Zone VLAN using corresponding VLAN name	String
8	service	.	
9	service service_custom	Name of the custom service for which a rule is to be added. Custom name should already be added into custom service	String
10	service service_normal	Name of the service for which a rule is to be added.	Service type.
11	action	Action to be taken by the rule.	Firewall rule action type.
12	schedule	Name of schedule for which the rule is applicable.	String.
13	source_address_type	Type of the source user.	Firewall rule address type.
14	destination_address_type	Type of the destination user.	Firewall rule address type.
15	snat_address_type	Type of the SNAT address.	Firewall rule snat address type.
16	log	Log Always or Never	Firewall rule log enable/disable.
17	source_address_start	IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
18	source_address_end	IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
19	destination_address_start	IP of the Destination user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
20	destination_address_end	IP of the Destination user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
21	qos_priority	Firewall type of service.	firewall type of service
22	wan_interface	WAN interface for Source NAT settings.	WAN interface type
23	snat_address	IP of the SNAT Address.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
24	alias_SNAT_ipaddress	Set Ip to use alias as Internal_Interface for firewall.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
25	dnat_port	The port number to use for DNAT, required if port forwarding is enabled.	Port number
26	port_forwarding_enable	Enables/disables port forwarding based on this firewall rule configuration settings.	Boolean choice
27	internal_ip_address	Sends to Local Server (DNAT IP), Specifies an IP address and port number of a machine on the Local Network which is hosting the server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
28	dnat_ipaddress	Sets it as Dedicated/configured WAN/3G WAN.	WAN interface type
29	alias_DNAT_ipaddress	Sets Ip to use alias as External_Interface for firewall.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12.10 security firewall ipv4 default_outbound_policy *<default_outbound_policy>*

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

12.11 security firewall ipv4 edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Firewall IPV4 rules configuration mode.	Unsigned integer
2	save	Saves Firewall IPV4 rules configuration settings.	
3	exit	Saves Firewall IPV4 rules configuration settings and exit current mode.	
4	cancel	To revert to the previous IPV4 rules configuration settings.	
5	from_zone	Sets from Zone security type.	Firewall rule type.
6	from_zone_vlan	Sets From Zone VLAN using corresponding VLAN name.	String
7	to_zone	Sets to Zone security type.	Firewall rule type.
8	to_zone_vlan	Sets To Zone VLAN using corresponding VLAN name.	String
9	service	.	
10	service service_custom	Name of the custom service for which a rule is to be added. Custom name should already be added into custom service.	String
11	service service_normal	Name of the service for which a rule is to be added.	Service type.
12	action	Action to be taken by the rule.	Firewall rule action type.
13	schedule	Name of schedule for which the rule is applicable.	String
14	source_address_type	Type of the source user.	Firewall rule address type.
15	destination_address_type	Type of the destination user.	Firewall rule address type.
16	snat_address_type	Type of the SNAT address.	Firewall rule snat address type.
17	log	Log Always or Never.	Firewall rule log enable/disable.
18	source_address_start	IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
19	source_address_end	IP of the Source user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

S.No	Command Name	Description	Type and Description
20	destination_address_start	IP of the Destination user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
21	destination_address_end	IP of the Destiation user.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
22	qos_priority	Firewall type of service.	Firewall type of service.
23	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 where each part is in the range 0-255.
25	alias_SNAT_ipaddress	Sets Ip to use alias as Internal_Interface for firewall.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
26	dnat_port	The port number to use for DNAT, required if port forwarding is enabled.	Port number.
27	port_forwarding_enable	Enables/disables port forwarding based on this firewall rule configuration settings.	Boolean choice.
28	internal_ip_address	Send to Local Server (DNAT IP), Specifies an IP address and port number of a machine on the Local Network which is hosting the server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.
29	dnat_ipaddress	Sets it as Dedicated/configured WAN/3G WAN.	WAN interface type.
30	alias_DNAT_ipaddress	Sets Ip to use alias as External_Interface for firewall.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255.

12.12 security firewall ipv4 enable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Enables Firewall IPv4 rules configuration mode.	Unsigned integer

12.13 security firewall ipv4 disable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Disables Firewall IPv4 Rules configuration mode.	Unsigned integer

12.14 security firewall ipv4 delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes a specified Firewall IPV4 Rule.	Unsigned integer

12.15 security firewall ipv4 move *<row_id>*

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

12.16 security firewall algs

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

S.No	Command Name	Description	Type and Description
7	Tftp	Protocal to be enabled at ALGs.	Boolean choice

12.17 security firewall ipv6 configure

S.No	Command Name	Description	Type and Description
1	save	Saves Firewall IPV6 rules configuration settings.	
2	exit	Saves Firewall IPV6 rules configuration settings and exit current mode.	
3	cancel	To revert to the previous IPV6 rules configuration settings.	
4	rule_type	Type of rule to be added.	Firewall rule type.
5	service	.	
6	service service_custom	Name of the custom service for which a rule is to be added; custom name should already be added into custom service.	String
7	service service_normal	Name of the service for which a rule is to be added.	Service type.
8	action	Action to be taken by the rule.	Firewall rule action type.
9	schedule	Schedule for which the rule is applicable.	String
10	source_address_type	Type of the source user.	Firewall rule address type.
11	destination_address_type	Type of the destination user.	Firewall rule address type.
12	log	Log Always or Never.	Firewall rule log enable/disable.
13	source_start_address	Start IP address 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:].
14	source_end_address	End IP address 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

S.No	Command Name	Description	Type and Description
16	destination_start_address	Start IP address 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	End IP address of the Destiation 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

12.18 security firewall ipv6 edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Firewall IPV6 rules configuration mode.	Unsigned integer
2	save	Saves Firewall IPV6 rules configuration settings.	
3	exit	Saves Firewall IPV6 rules configuration settings and exit current mode.	
4	cancel	To revert to the previous IPV6 rules configuration settings.	
5	rule_type	Type of rule to be added.	firewall rule type
6	service	.	
7	service service_custom	Name of the custom service for which a rule is to be added custom name should already be added into custom service.	String
8	service service_normal	Name of the service for which a rule is to be added.	Service type.
9	action	Action to be taken by the rule.	Firewall rule action type.
10	schedule	Schedule for which the rule is applicable.	String
11	source_address_type	Type of the source user.	Firewall rule address type.
12	destination_address_type	Type of the destination user.	Firewall rule address type.
13	log	Log Always or Never.	Firewall rule log enable/disable.
14	source_start_address	Start IP of the Source user.	IP address abcd:abcd:abcd:abcd:abcd:abc

S.No	Command Name	Description	Type and Description
			d:abcd:abcd where each part is in the range [0-9A-Fa-f:]
15	source_end_address	End 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	Start IP of the Destination user.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
18	destination_end_address	End IP of the Destiation user.	IP address abcd:abcd: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

12.19 security firewall ipv6 enable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Enables selected Firewall IPV6 rule.	Unsigned integer

12.20 security firewall ipv6 disable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Disables selected Firewall IPV6 Rule.	Unsigned integer

12.21 security firewall ipv6 delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes selected Firewall IPV6 Rule.	Unsigned integer

12.22 security firewall ipv6 move *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Firewall IPV6 Rule reordering mode.	Row id(s) a,b,c where each part is a valid rowid in the range [0-9]

S.No	Command Name	Description	Type and Description
2	save	Saves Firewall IPV6 rule reordering settings.	
3	exit	Saves Firewall IPV6 rule reordering settings and exit current mode.	
4	cancel	To revert to the previous IPV6 rule reordering settings.	
5	position	New position for the rule.	Unsigned integer

12.23 security firewall ipv6 default_outbound_policy *<default_outbound_policy>*

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

12.24 security ids configure

S.No	Command Name	Description	Type and Description
1	save	Saves IDS configuration settings.	
2	exit	Saves IDS configuration settings and exit current mode.	
3	cancel	To revert to the previous IDS configuration settings.	
4	enable	Enables Intrusion detection system.	Boolean choice
5	intrusion_log_enable	Enables/Disables intrusion logs.	Boolean choice

12.25 security session_settings configure

S.No	Command Name	Description	Type and Description
1	save	Saves security session settings configuration settings.	

S.No	Command Name	Description	Type and Description
2	exit	Saves session settings configuration settings and exit current mode.	
3	cancel	To revert to the previous session settings configuration settings.	
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

12.26 security schedules add

S.No	Command Name	Description	Type and Description
1	save	Saves schedules configuration settings.	
2	exit	Saves schedules configuration settings and exit current mode.	
3	cancel	To revert to the previous schedules configuration settings.	
4	name	Name of the schedule for which a rule is to be added.	String
5	days	The days when the schedule is active.	
6	days all	The schedule applies to all days. This option is the default selection.	Boolean choice
7	days monday	Checks the box for each day to include in this schedule.	Boolean choice
8	days tuesday	Checks the box for each day to include in this schedule.	Boolean choice

S.No	Command Name	Description	Type and Description
9	days wednesday	Checks the box for each day to include in this schedule.	Boolean choice
10	days thursday	Checks the box for each day to include in this schedule.	Boolean choice
11	days friday	Checks the box for each day to include in this schedule.	Boolean choice
12	days saturday	Checks the box for each day to include in this schedule.	Boolean choice
13	days sunday	Checks the box for each day to include in this schedule.	Boolean choice
14	time_of_day	Scheduled time of day.	
15	time_of_day all_enable	Selects type of schedule activation for time of the day.	Boolean choice
16	time_of_day start	The start time for the schedule.	
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	The end time for the schedule.	
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.

12.27 security schedules edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Schedules configuration mode.	Unsigned integer
2	save	Saves schedules configuration settings.	

S.No	Command Name	Description	Type and Description
3	exit	Saves schedules configuration settings and exit current mode.	
4	cancel	To revert to the previous schedules configuration settings.	
5	name	Name of the schedule for which a rule is to be added	String
6	days	The days when the schedule is active.	
7	days all	The schedule applies to all days. This option is the default selection.	Boolean choice
8	days monday	Checks the box for each day to include in this schedule.	Boolean choice
9	days tuesday	Checks the box for each day to include in this schedule.	Boolean choice
10	days wednesday	Checks the box for each day to include in this schedule.	Boolean choice
11	days thursday	Checks the box for each day to include in this schedule.	Boolean choice
12	days friday	Checks the box for each day to include in this schedule.	Boolean choice
13	days saturday	Checks the box for each day to include in this schedule.	Boolean choice
14	days sunday	Checks the box for each day to include in this schedule.	Boolean choice
15	time_of_day	Scheduled time of day.	
16	time_of_day all_enable	Selects the type of schedule activation for time of the day.	Boolean choice
17	time_of_day start	The start time for the schedule.	
18	time_of_day start mins	Minutes	Minute in the format MM(00-59).
19	time_of_day start hours	Hours	Schedule time unit type.

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

12.28 security schedules delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes the selected schedule or schedules.	Unsigned integer

12.29 security firewall smtpAlg configure

S.No	Command Name	Description	Type and Description
1	Save	Saves SmtpAlg configuration settings.	
2	Exit	Saves SmtpAlg configuration settings and exit current mode.	
3	cancel	To revert to the previous SmtpAlg configuration settings.	
4	smtp_Alg_Status	Enables/disables SmtpAlg status.	Boolean choice
5	port	Sets the port you want to use for Smtp Alg.	Unsigned integer

12.30 security firewall smtpAlg approvedMailId add

S.No	Command Name	Description	Type and Description
1	save	Saves ApprovedMailId configuration settings.	
2	exit	Saves ApprovedMailId configuration settings and exit current mode.	

S.No	Command Name	Description	Type and Description
3	cancel	To revert to the previous ApprovedMailId configuration settings.	
4	approved_Mail_Id	Approved Mail_Id	String

12.31 security firewall smtpAlg approvedMailId edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	It allows to edit an approved MailId.	Unsigned integer
2	save	Saves ApprovedMailId configuration settings.	
3	exit	Saves ApprovedMailId configuration settings and exit current mode.	
4	cancel	To revert to the previous ApprovedMailId configuration settings.	
5	approved_Mail_Id	Approved Mail_Id	String

12.32 security firewall smtpAlg approvedMailId delete *<row_id>*

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

12.33 security firewall smtpAlg blockedMailId add

S.No	Command Name	Description	Type and Description
1	save	Saves BlockedMailId configuration settings.	
2	exit	Saves BlockedMailId configuration settings and exit current mode.	
3	cancel	To revert to the previous BlockedMailId configuration settings.	
4	blocked_Mail_Id	Blocked Mail_Id	String

12.34 security firewall smtpAlg blockedMailId edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	It allows to edit a blocked MailId.	Unsigned integer
2	save	Saves BlockedMailId configuration settings.	
3	exit	Saves BlockedMailId configuration settings and exit current mode.	
4	cancel	To revert to the previous BlockedMailId configuration settings.	
5	blocked_Mail_Id	Blocked Mail_Id	String

12.35 security firewall smtpAlg blockedMailId delete *<row_id>*

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

12.36 security firewall smtpAlg subjectList add

S.No	Command Name	Description	Type and Description
1	save	Saves subjectList configuration settings.	
2	exit	Saves subjectList configuration settings and exit current mode.	
3	cancel	To revert to the previous subjectList configuration settings.	
4	subject	Subject in the Mail_Id.	String
5	mail_Id	Enter the Mail_Id.	String
6	action	Action Allow/Block.	Boolean choice

12.37 security firewall smtpAlg subjectList edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	It allows to edit subject with MailId and action.	Unsigned integer
2	save	Saves subjectList configuration settings.	
3	exit	Saves subjectList configuration settings and exit current mode.	
4	cancel	To revert to the previous subjectList configuration settings.	
5	subject	Subject in the Mail_Id.	String
6	mail_Id	Enter the Mail_Id.	String
7	action	Action Allow/Block.	Boolean choice

12.38 security firewall smtpAlg subjectList delete *<row_id>*

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

12.39 security mac_filter configure

S.No	Command Name	Description	Type and Description
1	save	Saves mac filter configuration settings.	
2	exit	Saves mac filter configuration settings and exit current mode.	
3	cancel	To revert to the previous mac filter configuration settings.	
4	enable	Enables/Disables the mac filter status.	Boolean choice
5	policy	Sets the mac address policy.	Policy type for mac addresses.

12.40 security mac_filter source add

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

12.41 security mac_filter source edit *<row_id>*

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

12.42 security mac_filter source delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes the selected Source Mac Filter configuration.	Unsigned integer

12.43 security ip_or_mac_binding add

S.No	Command Name	Description	Type and Description
1	save	Saves ip mac binding configuration settings.	
2	exit	Saves ip mac binding configuration settings and exit current mode.	
3	cancel	To revert to the previous ip mac binding configuration settings.	
4	computer_name	Specifies 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	Specifies logging option for this rule.	Boolean choice

12.44 security ip_or_mac_binding edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Ip/mac binding configuration mode.	Unsigned integer
2	save	Saves ip mac binding configuration settings.	
3	exit	Saves ip mac binding configuration settings and exit current mode.	
4	cancel	To revert to the previous ip mac binding configuration settings.	
5	computer_name	Specifies 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

S.No	Command Name	Description	Type and Description
8	log_dropped_packets	Specifies logging option for this rule.	Boolean choice

12.45 security ip_or_mac_binding delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes the selected ip/mac binding configuration.	Unsigned integer

12.46 security firewall vpn_passthrough configure

S.No	Command Name	Description	Type and Description
1	save	Saves VPN Passthrough configuration settings.	
2	exit	Saves VPN Passthrough configuration settings and exit current mode.	
3	cancel	To revert to the previous VPN Passthrough configuration settings.	
4	ipsec_enable	Enables or DisablesIPSEC Passthrough.	Boolean choice
5	pptp_enable	Enables or DisablesPPTP Passthrough.	Boolean choice
6	l2tp_enable	Enables or DisablesL2TP Passthrough.	Boolean choice

12.47 security webAccess status *<status>*

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

12.48 security webAccess add

S.No	Command Name	Description	Type and Description
1	save	Security webAccess configuration.	

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

12.49 security webAccess edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Security webAccess edit	Unsigned integer
2	save	Security webAccess configuration.	
3	exit	Saves webAccess rules configuration settings and exit current mode.	
4	cancel	To revert to the previous webAccess rules configuration settings.	
5	name	Name	String
6	accessType	AcessType	Access Type for web access filter
7	ipAddr	IpAddr	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	vlanId	VlanId	Number in the range 1-4095

12.50 security webAccess delete *<row_id>*

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

12.51 security website_filter content_filtering configure

S.No	Command Name	Description	Type and Description
1	save	Saves contentFiltering configuration settings.	
2	exit	Saves content Filtering configuration settings and exit current mode.	
3	cancel	To revert to the previous content filtering configuration settings.	
4	content_filtering	Enables/Disables content Filtering.	Boolean choice
5	proxy_enable	Enables/Disables proxy.	Boolean choice
6	java_enable	Enables/Disables java.	Boolean choice
7	activex_enable	Enables/Disables activex.	Boolean choice
8	cookies_enable	Enables/Disables cookies.	Boolean choice

12.52 security website_filter approved_urls add

S.No	Command Name	Description	Type and Description
1	save	Saves trusted domains configuration settings.	
2	exit	Saves trusted domains configuration settings and exit current mode.	
3	cancel	To revert to the previous trusted domains configuration settings.	
4	url	Trusted domain name.	String

12.53 security website_filter approved_urls edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Trusted domains configuration mode.	Unsigned integer
2	save	Saves trusted domains configuration settings.	

S.No	Command Name	Description	Type and Description
3	exit	Saves trusted domains configuration settings and exit current mode.	
4	cancel	To revert to the previous trusted domains configuration settings.	
5	url	Trusted domain name.	String

12.54 security website_filter approved_urls delete *<row_id>*

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

12.55 security website_filter blocked_keywords add

S.No	Command Name	Description	Type and Description
1	save	Saves blocked keywords configuration settings.	
2	exit	Saves blocked keywords configuration settings and exit current mode.	
3	cancel	To revert to the previous blocked keywords configuration settings.	
4	blocked_keyword	Enter keyword to be blocked.	String

12.56 security website_filter blocked_keywords edit *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Blocked Keywords configuration mode.	Unsigned integer
2	save	Saves blocked keywords configuration settings.	
3	exit	Saves blocked keywords configuration settings and exit current mode.	

S.No	Command Name	Description	Type and Description
4	cancel	To revert to the previous blocked keywords configuration settings.	
5	blocked_keyword	Enter keyword to be blocked.	String

12.57 security website_filter blocked_keywords delete *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Deletes the selected Blocked Keywords.	Unsigned integer

12.58 security website_filter blocked_keywords enable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Enables the selected Blocked Keywords.	Unsigned integer

12.59 security website_filter blocked_keywords disable *<row_id>*

S.No	Command Name	Description	Type and Description
1	*<row_id>*	Disables the selected Blocked Keywords.	Unsigned integer