D-Link®
Building Networks for People

Unified Services Router CLI Reference Guide

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

Release 1.04

Small Business Gateway Solution http://security.dlink.com

CLI Reference Guide

Unified Services Router

D-Link Corporation

http://www.dlink.com

CLI Reference Guide
DSR-250/250N/500/500N/1000/1000N
Unified Services Router
Version 1.04

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-1000N/1000/500N/500/250N/250 series of routers.

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

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

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

1.1 Accessing the CLI

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

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

 Welcome to the DSR Command Line Interface

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

D-Link DSR>
```

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

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

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

Chapter 2. Basic commands available on the CLI

2.1 CONTEXT SENSITIVE HELP

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

2.2 AUTO-COMPLETION

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

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

2.3 MOVEMENT KEYS

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

2.4 DELETION KEYS

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

2.5 ESCAPE SEQUENCES

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

Chapter 3. Command Hierarchy in CLI

3.1 CLI commands can be divided into 4 categories:

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

3.2 The router configuration is divided into 5 branches:

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

Chapter 4. Global commands used in CLI

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

Chapter 5. Show commands used in CLI

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

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

Sl No	Command Name	Purpose
1	show net available_lan_host list	Display available lan host list
2	show net bandwidth profile setup	Display bandwidth profile configuration
3	show net ddns setup	Display ddns configuration
4	show net dhcp leased_clients list	Display dhcp leased clients list
5	show net dhcp reserved_ip setup	Display dhcp reserved ip configuration
6	show net routing dynamic setup	Display dynamic routing configuration
7	show net mode setup	Display network mode configuration
8	show net ipv6_tunnel setup	Display ipv6 tunnel's configuration
9	show net lan ipv4 setup	Display ipv4 lan configuration
10	show net port management setup	Display port management configuration
11	show net radvd setup	Display radvd configuration
12	show net routing mode setup	Display routing mode configuration
13	show net routing static ipv4 setup	Display ipv4 static routes configuration
14	show net routing static ipv6 setup	Display ipv6 static routes configuration
15	show net statistics	Display network statistics
16	show net bandwidth traffic_selector setup	Display bandwidth traffic selector configurations
17	show net upnp portmap	Display upnp portmap
18	show net upnp setup	Display upnp configuration
19	show net wan wan1 ipv4 setup	Display ipv4 wan1 configuration
20	show net wan wan1 ipv4 status	Display ipv4 wan1 connection status
21	show net wan wan2 ipv4 setup	Display ipv4 wan2 configuration
22	show net ddns setup	Display ddns configuration for dedicated WAN and configurable WAN
23	show net routing protocol_binding setup	Display protocol binding configuration
24	show net dmz dhcp reserved_ip setup	Display dhcp reserved ip configuration

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

Sl No	Command Name	Purpose
1	show security attack_checks setup	Display Security Checks configuration
2	show security blocked_keywords setup	Display blocked keywords configuration
3	show security content_filtering setup	Display content filtering configuration
4	show security custom_service setup	Display Custom Service configuration
5	show security firewall ipv4 setup	Display Firewall Rules
6	show security firewall ipv6 setup	Display Firewall Rules
7	show security ids setup	Display IDS configuration
8	show security ip_or_mac_binding setup	Display IP/MAC Binding configuration
9	show security port_triggering setup	Display Port Triggering configuration
10	show security schedules setup	Display Schedules configuration
11	show security session_settings	Display Session Settings configuration
12	show security mac_filter setup	Display Source Mac Filter configuration
13	show security trusted_domains setup	Display trusted domains configuration
14	show security vpn_passthrough setup	Display VPN passthrough Configuration

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

Sl No	Command Name	Purpose
1	show system logging ipv6 setup	Display logging configuration
2	show system logging facility setup	Display logging facility configuration
3	show system logging ipv4 setup	Display logging configuration
4	show system radius setup	Display radius configuration
5	show system logging remote setup	Display remote logging configuration
6	show system remote_management setup	Display Remote Management configuration
7	show system snmp setup	Display snmp configuration
8	show system status	Display system status
9	show system time setup	Display timezone and ntp configuration
10	show system traffic_meter setup	Display traffic meter 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:

Sl No	Command Name	Purpose
1	show dot11 access point setup [ap_name]	Display access point configuration
2	Show dot11 radio setup	Display radio configuration

Sl No	Command Name	Purpose
3	Show dot11 profile setup [profile_name] [display_qos]	Display profile 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:

Sl No	Command Name	Purpose
1	show vpn ipsec dhcp setup	Show DHCP setup
2	show vpn ipsec policy setup	Show list of ipsec policies
3	show vpn ipsec policy status	Show the status of policies
4	show vpn sslvpn client	Show SSLVPN client settings
5	show vpn sslvpn policy	Show SSLVPN policy settings
6	show vpn sslvpn portal-layouts	Show SSLVPN portal layout settings
7	show vpn sslvpn portforwarding appconfig	Show SSLVPN port forwarding application configuration
8	show vpn sslvpn portforwarding hostconfig	Show SSLVPN port forwarding host configuration
9	show vpn sslvpn resource	Show SSLVPN resource settings
10	show vpn sslvpn resource-object	Show SSLVPN resource objects
11	show vpn sslvpn route	Show SSLVPN configured client routes
12	Show vpn sslv[n users users	Show List of Users
13	show vpn sslvpn users domains	Show List od Domains
14	show vpn sslvpn users groups	Show List of Groups
15	show vpn sslvpn users browser_policies	Show List of Browser Policies
16	show vpn sslvpn users ip_policies	Show List of IP Policies
17	show vpn sslvpn users login_policies	Show List of Login Policies

Chapter 6. Utility commands used in CLI

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

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

6.1 util ping <ip_address>

Sl No	Command Name	Description	Type and Description
1	ip_address	Ping target IP address.	IP Address, Ping target IP address.

6.2 util system_check capturePackets

Sl No	Command Name	Description	Type and Description
1	download	Download the packet capture to the host machine	Download the packet capture to the host machine
2	Start	Start the packet capture	Specify the interface (WAN1, WAN2 and LAN)
3	Stop	Stop the packet capture	

6.3 util system_check

Sl No	Command Name	Description	Type and Description
1	display_IPV4_routingtable	Display IPV4 Routing Table	Display IPV4 Routing Table

6.4 util system_check dns_lookup

Sl No	Command Name	Description	Type and Description
1	dns	Internet name	String IP address DNS

6.5 util system_check traceroute

Sl No	Command Name	Description	Type and Description
1	ip_address	It displays all the routers present	String

Sl No	Command Name	Description	Type and Description
		between the destination IP address and this router	IP address

Chapter 7. Configure commands used in CLI

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

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

Sl No	Command Name	Purpose
1	net bandwidth profile add	It allows to add a bandwidth profile.
2	net bandwidth profile edit	It allows to edit a bandwidth profile.
3	net bandwidth profile delete	It allows to delete a bandwidth profile.
4	net ddns configure	Ddns configuration mode
5	net routing dynamic configure	Dynamic routing configuration mode
6	net mode configure	IP Mode configuration mode
7	net ipv6_tunnel isatap add	Isatap tunnel configuration mode.
8	net ipv6_tunnel isatap delete	Delete the configured isatap tunnel
9	net ipv6_tunnel isatap edit	Isatap tunnel configuration mode.
10	net ipv6_tunnel six_to_four automatic_tunneling enable	Six to four tunnel configuration mode
11	net lan dhcp reserved_ip add	Dhcp reserved ip configuration mode
12	net lan dhcp reserved_ip delete	Delete the configured dhcp reserved ip
13	net lan ipv4 configure	Lan configuration mode
14	net lan ipv6 configure	Lan configuration mode
15	net lan ipv6 pool configure	Ipv6 pool configuration mode
17	net mld configure	MLD configuration mode
18	net port management configure	Port management configuration mode
19	net radvd configure	Radvd configuration mode
20	net radvd pool add	Radvd pool configuration add mode
21	net radvd pool delete	Radvd pool configuration delete mode
22	net radvd pool edit	Radvd pool configuration edit mode
23	net routing mode configure	Routing mode configuration
24	net routing static ipv4 configure	Static route configuration mode
25	net routing static ipv4 delete	Static route configuration delete mode
26	net routing static ipv6 configure	Static route configuration mode
27	net routing static ipv6 delete	Static route configuration delete mode
28	net bandwidth traffic_selector add	Traffic selector configuration mode

Sl No	Command Name	Purpose
29	net bandwidth traffic_selector edit	Traffic selector configuration edit mode
30	net bandwidth traffic_selector delete	Traffic selector configuration delete mode
31	net upnp configure	Upnp configuration mode
32	net wan wan1 ipv4 configure	Wan1 ipv4 configuration mode
33	net wan ipv6 configure	Wan ipv6 configuration mode
34	net wan wan2 ipv4 configure	Wan2 ipv4 configuration mode
35	net wan wan1-pppoeprofile	Wan1 profile configuration mode
36	net wan wan2-pppoeprofile	Wan2 profile 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:

Sl No	Command Name	Purpose
1	security attack_checks configure	security checks configuration mode.
2	security blocked_keywords add	blocked Keyword configuration mode.
3	security blocked_keywords disable	blocked Keyword configuration mode.
4	security blocked_keywords delete	blocked Keyword configuration mode.
5	security blocked_keywords edit	blocked Keyword configuration mode.
6	security blocked_keywords enable	blocked Keyword configuration mode.
7	security content_filtering configure	content filtering configuration mode.
8	security custom_service add	custom service configuration mode.
9	security custom_service delete	custom service configuration mode.
10	security custom_service edit	custom service configuration mode.
11	security firewall ipv4 default_outbound_policy enable	Firewall Settings, Default Outbound Policy configuration mode.
12	security firewall ipv6 default_outbound_policy enable	Firewall Settings, Default Outbound Policy configuration mode.
13	security firewall ipv4 configure	Firewall IPV4 rules configuration mode.
14	security firewall ipv4 delete	Firewall IPV4 rules configuration mode.
15	security firewall ipv4 disable	Firewall IPV4 rules configuration mode.
16	security firewall ipv4 edit	Firewall IPV4 rules configuration mode.
17	security firewall ipv4 enable	Firewall IPV4 rules configuration mode.
18	security firewall ipv6 configure	Firewall IPV6 rules configuration mode.
19	security firewall ipv6 delete	Firewall IPV6 rules configuration mode.
20	security firewall ipv6 disable	Firewall IPV6 rules configuration mode.
21	security firewall ipv6 edit	Firewall IPV6 rules configuration mode.
22	security firewall ipv6 enable	Firewall IPV6 rules configuration mode.

Sl No	Command Name	Purpose
23	security ids configure	IDS configuration mode
24	security ip_or_mac_binding add	IP/Mac Binding configuration mode
25	security ip_or_mac_binding delete	IP/Mac Binding configuration mode.
26	security ip_or_mac_binding edit	IP/Mac Binding configuration mode.
27	security port_triggering add	port triggering rules configuration mode.
28	security port_triggering delete	port triggering rules configuration mode.
29	security port_triggering edit	port triggering rules configuration mode.
30	security schedules add	Schedules configuration mode.
31	security schedules edit	Schedules configuration mode.
32	security schedules delete	Schedules configuration mode.
33	security session_settings configure	Session Settings configuration mode.
34	security mac_filter source add	Source Mac Filter configuration mode.
35	security mac_filter source delete	Source Mac Filter configuration mode.
36	security mac_filter source edit	Source Mac Filter configuration mode.
37	security mac_filter configure	Source Mac Filter configuration mode.
38	security trusted_domain add	trusted domains configuration mode.
39	security trusted_domain delete	trusted domains configuration mode.
40	security trusted_domain edit	trusted domains configuration mode.
41	security vpn_passthrough configure	VPN Passthrough configuration mode.

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

Sl No	Command Name	Purpose
1	system logging facility configure <facility_type>	Facility logging configuration mode
2	system logging ipv4 configure	Firewall ipv4 logs configuration mode
3	system logging ipv6 configure	Firewall ipv6 logs configuration mode
4	system logging remote configure	Remote logging configuration mode
5	system radius configure <radius_server>	Radius configuration mode
6	system radius delete <radius_server>	Radius configuration delete mode
7	system remote_management https configure	Remote management configuration mode
8	system snmp sys configure	Snmp system configuration mode
9	system snmp trap configure <agent_ip>	Snmp trap configuration mode
10	system snmp trap delete <agent_ip>	Snmp trap configuration delete mode
11	system time configure	Ntp time configuration mode
12	system traffic_meter configure	Traffic meter configuration mode

Sl No	Command Name	Purpose
13	system users idle_timeout <timeout>	Admin idle timeout configuration
14	system users password <user_string>	Users password configuration

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

Sl No	Command Name	Purpose
1	vpn ipsec policy connect	Command used to establish vpn connection
2	vpn ipsec policy drop	Command used to drop vpn connection
3	vpn ipsec policy configure	Command used to configure vpn policy (It may be auto or manual)
4	vpn ipsec policy delete	Command to delete vpn policy
5	vpn ipsec policy enable	Command to enable vpn policy
6	vpn ipsec policy disable	Command to disable vpn policy
7	vpn ipsec dhcp configure	Command to configure DHCP
8	vpn sslvpn client	SSLVPN Client configuration mode
9	vpn sslvpn policy add	SSLVPN policy add mode
10	vpn sslvpn policy edit	SSLVPN policy edit mode
11	vpn sslvpn policy delete	SSLVPN policy delete mode
12	vpn sslvpn portal-layouts add	SSLVPN portal layout add mode
13	vpn sslvpn portal-layouts edit	SSLVPN portal layout edit mode
14	vpn sslvpn portal-layouts delete	SSLVPN portal layout delete mode
15	vpn sslvpn portal-layouts set-default	SSLVPN portal layout set default mode
16	vpn sslvpn portforwarding appconfig add	SSLVPN application configuration add rule mode
17	vpn sslvpn portforwarding appconfig delete	SSLVPN application configuration delete rule mode
18	vpn sslvpn portforwarding hostconfig add	SSLVPN host configuration add rule mode
19	vpn sslvpn portforwarding hostconfig delete	SSLVPN host configuration delete rule mode
20	vpn sslvpn resource add	SSLVPN resource add mode
21	vpn sslvpn resource delete	SSLVPN resource delete mode
22	vpn sslvpn resource configure add	SSLVPN resource object add mode
23	vpn sslvpn resource configure delete	SSLVPN resource object delete mode
24	vpn sslvpn route add	SSLVPN client route add mode
25	vpn sslvpn route delete	SSLVPN client route delete mode
26	vpn sslvpn users users add	Users add mode
27	vpn sslvpn users users edit	Users edit mode
28	vpn sslvpn users users delete	Users delete mode
29	vpn sslvpn users domains add	Domains add mode

Sl No	Command Name	Purpose
30	vpn sslvpn users domains edit	Domains edit mode
31	vpn sslvpn users domains delete	Domains delete mode
32	vpn sslvpn users groups add	Groups add mode
33	vpn sslvpn users groups edit	Groups edit mode
34	vpn sslvpn users groups delete	Groups delete mode
35	vpn sslvpn users users ip_policies configure	Ip policies configure mode
36	vpn sslvpn users users ip_policies delete	Ip policies delete mode
37	vpn sslvpn users users browser_policies	Browser policies configuration mode
38	vpn sslvpn users users login_policies	Login policies configuration mode

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

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

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

Chapter 8. Configuration commands under branch NET

8.1 net bandwidth profile enable

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

8.2 net bandwidth profile add/edit

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

8.3 net bandwidth profile delete <row_id>

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

8.4 net ddns configure

Sl No	Command Name	Description	Type and Description
1	enable	Enable or disable Dyndns to provide Dynamic DNS service	Boolean (Y/N) Enable/ Disable DDNS service
2	hostname	Set Hostname	String Host name
3	username	Set username.	String Username.
4	password	Set Password.	String

Sl No	Command Name	Description	Type and Description
			Password.
5	wild_flag_enable	Enable / Disable using wild cards	Boolean (Y/N) Wildcard flag
6	time_update_enable	Set Timeperiod as 30 days	Boolean (Y/N) Update for every 30 days or not
7	cancel	Roll back DDNS configuration changes	
8	exit	Save DDNS configuration changes and exit current mode	
9	save	Save DDNS configuration changes	

8.5 net ipv6_tunnel isatap add/edit

Sl No	Command Name	Description	Type and Description
1	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.	Local end point address type (LAN/Other_IP),
2	ipv4_address	The local end point address if not the LAN IPv4 address	IP Address The local end point address
3	subnet_prefix	This is the 64-bit subnet prefix that is assigned to the logical	String, subnet prefix
4	cancel	Roll back isatap tunnel configuration changes.	
5	exit	Save isatap tunnel configuration changes and exit current mode.	
6	save	Save isatap tunnel configuration changes.	

8.6 net ipv6_tunnel isatap delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row Id of the tunnel to be deleted	Unsigned integer Row id number

8.7 net ipv6_tunnel six_to_four configure

Sl No	Command Name	Description	Type and Description
1	automatic_tunneling_enable	Enable/disable automatic tunneling which will allow traffic from an IPv6 LAN to be tunneled through a IPv4 WAN to reach an IPv6 network	Boolean (Y/N) Enable/ Disable automatic tunneling

8.8 net lan dhcp reserved_ip add

Sl No	Command Name	Description	Type and Description
1	mac_address	Reserved mac address used to add/edit	MAC address Reserved Mac address you want to add/edit
2	ip_address	IP Address to be reserved	IP Address IP Address to be reserved
3	cancel	Roll back DHCP Reserved IPs configuration changes	
4	exit	Save DHCP Reserved IPs configuration changes and exit current mode	
5	save	Save DHCP Reserved IPs configuration changes	

8.9 net lan dhcp reserved_ip delete <mac_address>

Sl No	Command Name	Description	Type and Description
1	mac_address	Reserved mac address used to delete	MAC address Reserved Mac address you want to delete

8.10 net lan group add <name>

Sl No	Command Name	Description	Type and Description
1	name	Unique groups name String	String, Group name

8.11 net lan group delete <name>

Sl No	Command Name	Description	Type and Description
1	name	Unique groups name String	String, Group name

8.12 net lan host add/edit

Sl No	Command Name	Description	Type and Description
1	group_name	Name of the group to which host belongs	String group name
2	ip_address	ip address of the host	IP Address, IP Address of the host
3	cancel	Roll back lan host configuration changes	
4	exit	Save lan host configuration changes	

Sl No	Command Name	Description	Type and Description
		and exit current mode	
5	save	Save lan host configuration changes	

8.13 net lan host delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	row id of lan host to be deleted	Unsigned integer Row id number

8.14 net lan ipv4 configure

Sl No	Command Name	Description	Type and Description
1	static address	Set system LAN IP address.	IP Address, System lan address
2	save	Save LAN configuration changes	

8.15 net lan ipv6 configure

Sl No	Command Name	Description	Type and Description
1	static address	Set system LAN IP address.	IP address, System lan ipv6 address
2	static prefix_length	Set prefix length.	Integer, Prefix length
3	dhcp domain_name	Set DHCP Server's Domain Name.	String, Domain name
4	dhcp rebind_time	Set system Lease Time.	Integer, number in range of 0 to 604800
5	dhcp mode	Set dhcpv6 mode.	Dhcp mode type, Stateless/Stateful
6	dhcp dns_type	Set dns server type	Dns server types, useDnsProxy/useDnsFromISP/use EnteredDns
7	dhcp primary_dns	Set primary dns server.	IP Address, Primary dns address
8	dhcp secondary_dns	Set secondary dns server.	IP Address, Secondary dns address
9	dhcp server_enable	Set dhcpv6 server status	Dhcp server status, Boolean Choice (Y/N)
10	dhcp server_preference	server preference number	Integer, Dhcp server preference number
11	cancel	Roll back LAN configuration changes	
12	exit	Save LAN configuration changes and exit current mode	

Sl No	Command Name	Description	Type and Description
13	save	Save LAN configuration changes	

8.16 net lan ipv6 pool configure <start_address>

Sl No	Command Name	Description	Type and Description
1	start_address	Set dhcpv6 start IP address.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range
2	end_address	Set dhcpv6 end IP address.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range
3	prefix	Set dhcpv6 prefix length.	Unsigned integer, Prefix length
4	cancel	Roll back ipv6 pool configuration changes	
5	exit	Save ipv6 pool configuration changes and exit current mode	
6	save	Save ipv6 pool configuration changes	

8.17 net lan ipv6 pool delete <start_address>

Sl No	Command Name	Description	Type and Description
1	start_address	Set dhcpv6 start IP address.	IP address abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range

8.18 net mode configure

Sl No	Command Name	Description	Type and Description
1	ip_type	Select IPv4 only or IPv4/IPv6 mode.	Ip mode type, IPv4 only or IPv4 and IPv6.
2	cancel	Roll back mode configuration changes	
3	exit	Save mode configuration changes and exit current mode	
4	save	Save mode configuration changes	

8.19 net port management configure <port_name>

Sl No	Command Name	Description	Type and Description
1	port_name	port name LAN/WAN to manage dedicated port's	Port name, Port1-LAN/Port2-WAN
2	auto_negotiation_enable	Select this to let the gateway and network to determine the optimal port settings.	Boolean Choice (Y/N) Enable/disable auto negotiation option,
3	duplex_mode	Choose between Half Duplex and Full Duplex based on the port support. The default is Full Duplex for all ports.	Duplex mode type, Half or full
4	enable	Enable/Disable the port status	Boolean choice (Y/N), Port status enable/disable
5	speed	One of three port speeds can be selected: 10 Mbps, 100 Mbps and 1000 Mbps (i.e. 1 Gbps). The de fault setting is 1000 Mbps for all ports	Port speed type, 10/100/1000
6	cancel	Roll back port management configuration changes	
7	exit	Save port management configuration changes and exit current mode	
8	save	Save port management configuration changes	

8.20 net radvd configure

Sl No	Command Name	Description	Type and Description
1	enable	Enable the RADVD process here to allow stateless auto configuration of the IPv6 LAN network	Boolean choice (Y/N), Radvd status
2	life_time	The lifetime in seconds of the route. The default is 3600 seconds.	Integer, Advertisement Lifetime
3	mode	select N to send router advertisements (RA's) to all interfaces else Y	Boolean Choice (Y/N), Advertisement mode status
4	mtu	This is used in RA's to ensure all nodes on the network use the same MTU value in the cases where the LAN MTU is not well known. The default is 1500	Mtu size, It takes value between 1200 to 1500.
5	preference	Chose between low/medium/high for the preference associated with this router's RADVD process	Radvd preference type, Low/medium/high
6	flags managed_enable	Chose Managed to use the administered /stateful protocol for address auto configuration	Boolean choice (Y/N) Enable or disable the managed flag
7	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 (Y/N), Enable or disable other flags

Sl No	Command Name	Description	Type and Description
8	cancel	Roll back radvd configuration changes	
9	exit	Save radvd configuration changes and exit current mode	
10	Save	Save radvd configuration changes	

8.21 net radvd pool add/edit

Sl No	Command Name	Description	Type and Description
1	prefix_address	It specifies the IPv6 network address	prefix address, abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd where each part is in the range [0-9A-Fa-f:]
2	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	Integer, Prefix length
3	prefix_life_time	The length of time over which the requesting router is allowed to use the prefix	Integer, Life time value
4	prefix_type	Option whether to select the prefix type as 6to4 or Global/Local/ISATAP	IPv6 prefix type, 6To4/Global/Local/ISATAP
5	sla_id	The SLA ID (Site-Level Aggregation Identifier) in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent	Integer, Site-Level Aggregation Identifier
6	cancel	Roll back mode configuration changes	
7	exit	Save mode configuration changes and exit current mode	
8	save	Save mode configuration changes	

8.22 net radvd pool delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row Id of the multihoming entry to be deleted	Unsigned integer Row id number

8.23 net routing dynamic configure

Sl No	Command Name	Description	Type and Description
1	authentication_enable	Enable/Disable Authentication for RIP-2B/2M	Boolean Choice (Y/N) Authentication status for RIP-2B/2M
2	direction	rip direction None, In only, Out only, Both.	Rip direction type, None/In-only/Out-only/Both
3	ripng_enable	Enable/Disable the RIPNG functionality	Boolean Choice (Y/N)

Sl No	Command Name	Description	Type and Description
			Enable or disable ripng status
4	version	Rip version	Rip version type, Disabled/Rip1/Rip2B/Rip2M
5	first_key authentication_id	First MD5 Authentication Key	String, Alphanumeric md5 authentication key
6	first_key id_number	First MD5 Key Id	Integer, Unique md5 key identifier
7	first_key valid_from day	day in which md5 authentication key validity starts	Day in the format DD(01-31)
8	first_key valid_from hour	hour in which md5 authentication key validity starts	HH(00-23) using 24 hour clock
9	first_key valid_from minute	minute in which md5 authentication key validity starts	minute in the format MM(00-59)
10	first_key valid_from month	month in which md5 authentication key validity starts	Month in the format MM(01-12)
11	first_key valid_from second	second in which md5 authentication key validity starts	Second in the format SS(00-59)
12	first_key valid_from year	year in which md5 authentication key validity starts	Year , valid range is 1970 to 2037
13	first_key valid_to day	day in which md5 authentication key validity ends	Day in the format DD(01-31)
14	first_key valid_to hour	hour in which md5 authentication key validity ends	HH(00-23) using 24 hour clock
15	first_key valid_to minute	minute in which md5 authentication key validity ends	minute in the format MM(00-59)
16	first_key valid_to month	month in which md5 authentication key validity ends	Month in the format MM(01-12)
17	first_key valid_to first	first in which md5 authentication key validity ends	Second in the format SS(00-59)
18	first_key valid_to year	year in which md5 authentication key validity ends	Year , valid range is 1970 to 2037
19	second_key authentication_id	second MD5 Authentication Key	String, Alphanumeric md5 authentication key
20	second_key id_number	second MD5 Key Id	Integer, Unique md5 key identifier
21	second_key valid_from day	day in which md5 authentication key validity starts	Day in the format DD(01-31)
22	second_key valid_from hour	hour in which md5 authentication key validity starts	HH(00-23) using 24 hour clock
23	second_key valid_from minute	minute in which md5 authentication key validity starts	minute in the format MM(00-59)
24	second_key valid_from month	month in which md5 authentication key validity starts	Month in the format MM(01-12)

Sl No	Command Name	Description	Type and Description
25	second_key valid_from second	second in which md5 authentication key validity starts	Second in the format SS(00-59)
26	second_key valid_from year	year in which md5 authentication key validity starts	Year , valid range is 1970 to 2037
27	second_key valid_to day	day in which md5 authentication key validity ends	Day in the format DD(01-31)
28	second_key valid_to hour	hour in which md5 authentication key validity ends	HH(00-23) using 24 hour clock
29	second_key valid_to minute	minute in which md5 authentication key validity ends	minute in the format MM(00-59)
30	second_key valid_to month	month in which md5 authentication key validity ends	Month in the format MM(01-12)
31	second_key valid_to second	second in which md5 authentication key validity ends	Second in the format SS(00-59)
32	second_key valid_to year	year in which md5 authentication key validity ends	Year , valid range is 1970 to 2037
33	cancel	Roll back rip configuration changes.	
34	exit	Save dynamic routes changes and exit current mode.	
35	save	Save dynamic route changes.	

8.24 net routing mode configure

Sl No	Command Name	Description	Type and Description
1	cancel	Roll back routing mode configuration changes.	
2	exit	Save routing mode configuration changes and exit current mode.	
3	save	Save routing mode configuration changes.	
4	type	Select NAT or Classical Routing mode.	Routing mode type, NAT / Classical routing

8.25 net routing static ipv4 configure <name>

Sl No	Command Name	Description	Type and Description
1	name	Unique route name	String, Route name
2	active_flag	Defines whether its an active route	Boolean choice (Y/N), Set/unset the active flag
3	destination_address	Set the destination IP.	IP Address, Destination address
4	gateway_address	Set the gateway ip address	IP Address, Gateway address

Sl No	Command Name	Description	Type and Description
5	interface	Set interface for which the route is applied	String, Valid strings (LAN/WAN)
6	metric	Set the metric for this route	Integer value, Valid metric 2-15
7	private_flag	Defines whether the route can be shared with other gateways when RIP is enabled	Boolean Choice (Y/N), Set/unset the private flag
8	subnet_mask	Set the subnet for this rule.	IP address, Subnet mask
9	cancel	Roll back route configuration changes.	
10	exit	Save static routes changes and exit current mode.	
11	save	Save static route changes.	

8.26 net routing static ipv4 delete <name>

Sl No	Command Name	Description	Type and Description
1	name	Unique route name	String, Route name

8.27 net routing static ipv6 configure <name>

Sl No	Command Name	Description	Type and Description
1	name	Unique route name	String, Route name
2	active_flag	Defines whether its an active route	Boolean choice (Y/N), Set/unset the active flag
3	destination_address	Set the destination IP.	IP Address, Destination address
4	gateway_address	Set the gateway ip address	IP Address, Gateway address
5	interface	Set interface for which the route is applied	Interface type, Dedicated-WAN/LAN/6to4-WAN
6	metric	Set the metric for this route	Integer value, Valid metric 2-15
7	prefix	Set the prefix length for this rule.	Integer, Prefix length
8	cancel	Roll back route configuration changes.	
9	exit	Save static routes changes and exit current mode.	
10	save	Save static route changes.	

8.28 net routing static ipv6 delete <name>

Sl No	Command Name	Description	Type and Description
1	name	Unique route name	String, Route name

8.29 net upnp configure

Sl No	Command Name	Description	Type and Description
1	advertisement period	UPnP Advertisement Period	UPnP Advertisement Period. Valid range is 1 to 86400
2	advertisement time_to_live	Set Advertisement Time To Live (in seconds)	UPnP Advertisement Time To Live. Valid range is 1 to 255
3	Enable	Enable/Disable upnp	Boolean choice (Y/N), Upnp status
4	Cancel	Roll back upnp configuration changes	
5	exit	Save upnp configuration changes and exit current mode	
6	save	Save upnp configuration changes	

8.30 net wan mode configure

Sl No	Command Name	Description	Type and Description
1	wan_mode_type	Select which wan mode you want to select	Select among the options: SINGLE_WAN, LOAD_BALANCING, AUTO_ROLLOVER
2	loadbalancing algo	If Mode Type selected is LOAD_BALANCING, this field gives you options to configure LOAD_BALANCING credentials	Enter the type of LoadBalancing Algo : Round-Robbin or Spillover
3	loadbalancing spillover load_tolerance	Percentage of max bandwidth after which the router switches to secondary WAN	valid Load Tolerance value is between 20 to 80
4	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	valid Maximum Bandwidth value is between 512bps to 8192bps
5	loadbalancing failover_method type	Select the Fail Over detection method	Set detection Type from None(0) DNS-lookup-Using-WAN-DNS(1) DNS-lookup-Using-CUSTOM(2) Ping-IP-Addresses(3)
6	loadbalancing failover_method dns ipaddr_wan1	Set WAN1 DNS IP	Valid ip address, valid wan1 dns ip n load balancing mode
7	loadbalancing failover_method dns ipaddr_wan2	Set WAN2 DNS IP	Valid ip address, valid wan2 dns ip n load balancing mode

Sl No	Command Name	Description	Type and Description
8	loadbalancing failover_method dns ipaddr_wan3	Set WAN3 DNS IP	Valid ip address, valid wan3 dns ip n load balancing mode
9	loadbalancing failover_method ping ipaddr_wan1	Set WAN1 PING IP	Valid ip address, valid wan1 ip in load balancing mode
10	loadbalancing failover_method ping ipaddr_wan2	Set WAN2 PING IP	Valid ip address, valid wan2 ip n load balancing mode
11	loadbalancing failover_method ping ipaddr_wan3	Set WAN3 PING IP	Valid ip address, valid wan3 ip n load balancing mode
12	loadbalancing failover_method retry_interval	Set retry time	Valid value is between 5 to 999
13	loadbalancing failover_method retry_attempts	Set failover attempts	Valid value is between 2 to 999
14	rollover wan_port	Select the Auto rollover WAN port as a primary wan	Set Primary WAN Type options from wan1 or wan2 or wan3
15	rollover wan_port_Sec	Select the Auto rollover WAN port as a secondary wan	Set Secondary WAN Type options from wan1 or wan2 or wan3
16	rollover failover_method type	Select the Fail Over detection method	"Set detection Type from None(0) DNS-lookup-Using-WAN-DNS(1) DNS-lookup-Using-CUSTOM(2) Ping-IP-Addresses(3)
17	rollover failover_method dns ipaddr_wan1	Set WAN1 DNS IP	Valid ip address, valid wan1 dns ip n rollver mode
18	rollover failover_method dns ipaddr_wan2	Set WAN2 DNS IP	Valid ip address, valid wan2 dns ip n rollver mode
19	rollover failover_method dns ipaddr_wan3	Set WAN3 DNS IP	Valid ip address, valid wan3 dns ip in rollver mode
20	rollover failover_method ping ipaddr_wan1	Set WAN1 PING IP	Valid ip address, valid wan1 ip in rollver mode
21	rollover failover_method ping ipaddr_wan2	Set WAN2 PING IP	Valid ip address, valid wan2 ip in rollver mode
22	rollover failover_method ping ipaddr_wan3	Set WAN3 PING IP	Valid ip address, valid wan3 ip in rollver mode
23	rollover failover_method retry_interval	Set retry time	Valid value is between 5 to 999
24	rollover failover_method retry_attempts	Set failover attempts	Valid value is between 2 to 999
25	singleport wan_port	Set WAN Type which you want to choose	Select from wan1 or wan2 or wan3
26	Cancel	Roll back upnp configuration changes	
27	exit	Save upnp configuration changes and exit current mode	
28	save	Save upnp configuration changes	

8.31 net wan configurable_port configure

Sl No	Command Name	Description	Type and Description
1	port_name	Select the configurable port type	Select from the wan2 or dmz

8.32 net wan wan1 ipv4 configure

Sl No	Command Name	Description	Type and Description
1	dhcpc mac_address	This command allows you to set the MAC address.	MAC Address, Its format is XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 (inclusive) or an alphabetical letter between A and F (inclusive).
2	dhcpc mac_type	The default is set to Use Default Address. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then select either Use this computer's MAC address or select Use This MAC Address and manually enter in the MAC address expected by your ISP.	Types of mac address source, Use-Default-Mac/Use-This-Computers-Mac/Use-This-Mac
3	dhcpc hostname	Set hostname	String,setting Dhcp hostname
4	dhcpc get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
5	dhcpc primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
6	dhcpc secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
7	Isp require_login	Select this option if your connection type is one of PPPoE, PPTP or L2TP	Boolean Choice (Y/N), Set Y if your connection type is once of PPPoE, PPTP or L2TP otherwise N.
8	isp_connection_type	Select among the options: STATIC, DHCPC, PPPoE, PPTP, or L2TP	ISP Types. STATIC/DHCPC/PPPOE/PPTP/L2TP
9	l2tp connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
10	l2tp idle_time	Set idle timeout value	idle timeout value type. Valid range is 5 to 999
11	l2tp my_address	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
12	l2tp password	Enter the password to log in.	String, Alphanumeric password
13	l2tp secret	Enter the secret phrase to log into the server	String, Alphanumeric server secret phrase
14	l2tp server_address	IP address of the L2TP server	IP address AAA.BBB.CCC.DDD

Sl No	Command Name	Description	Type and Description
			where each part is in the range 0-255
15	l2tp username	Enter the username to log in	String, Alphanumeric username
16	l2tp split_tunnel	Set Split Tunnel Mode	Boolean Choice(Y/N)
17	L2tp get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
18	l2tp primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
19	l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
20	pptp connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
21	pptp idle_time	Set idle timeout value	idle timeout value type. Valid range is 5 to 999
22	pptp my_address	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
23	pptp password	Enter the password to log in.	String, Alphanumeric password
24	pptp server_address	IP address of the PPTP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
25	pptp username	Enter the username to log in	String, Alphanumeric username
26	pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
27	pptp primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
28	pptp secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
29	pptp mmpe_encryption	Set Mmpe Encryption	Boolean Choice (Y/N)
30	pppoe profile1	Enable first PPPOE profile	Boolean Choice (Y/N)
31	pppoe profile2	Enable second PPPOE profile	Boolean Choice (Y/N)
32	cancel	Roll back wan configuration changes	
33	exit	Save wan configuration changes and exit current mode	
34	save	Save wan configuration changes	

8.33 net wan wan2 ipv4 configure

Sl No	Command Name	Description	Type and Description
1	dhcpc mac_address	This command allows you to set the MAC address.	MAC Address, Its format is XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 (inclusive) or an alphabetical letter between A and F (inclusive).
2	dhcpc mac_type	The default is set to Use Default Address. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then select either Use this computer's MAC address or select Use This MAC Address and manually enter in the MAC address expected by your ISP.	Types of mac address source, Use-Default-Mac/Use-This-Computers-Mac/Use-This-Mac
3	l2tp idle_time	Set idle timeout value	idle timeout value type. Valid range is 5 to 999
4	l2tp my_address	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
5	l2tp password	Enter the password to log in.	String, Alphanumeric password
6	l2tp secret	Enter the secret phrase to log into the server	String, Alphanumeric server secret phrase
7	l2tp server_address	IP address of the L2TP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
8	l2tp username	Enter the username to log in	String, Alphanumeric username
9	l2tp split_tunnel	Set Split Tunnel Mode	Boolean Choice(Y/N)
10	L2tp get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
11	l2tp primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
12	l2tp secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
13	pptp connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
14	pptp idle_time	Set idle timeout value	idle timeout value type. Valid range is 5 to 999
15	pptp my_address	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
16	pptp password	Enter the password to log in.	String, Alphanumeric password
17	pptp server_address	IP address of the PPTP server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

Sl No	Command Name	Description	Type and Description
18	pptp username	Enter the username to log in	String, Alphanumeric username
19	pptp get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
20	pptp primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
21	pptp secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
22	pptp mmpe_encryption	Set Mmpe Encryption	Boolean Choice (Y/N)
23	pppoe profile1	Enable first PPPOE profile	Boolean Choice (Y/N)
24	pppoe profile2	Enable second PPPOE profile	Boolean Choice (Y/N)
25	threeg apn		
26	threeg authMethod	Setting Threeg authentication methods	authMethods like PAP/CHAP/NONE
27	threeg username	Enter the username to log in	String, Alphanumeric username
28	threeg password	Enter the password to log in	String, Alphanumeric password
29	threeg get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
30	threeg primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
31	threeg secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
32	threeg connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
33	threeg dial_number	Enter the number to dail in	String Type
34	Cancel	Roll back wan configuration changes	
35	Exit	Save wan configuration changes and exit current mode	
36	Save	Save wan configuration changes	

8.34 net wan wan3 threeG configure

Sl No	Command Name	Description	Type and Description
1	Username	Enter the username required to log in to the ISP	String, Alphanumeric username
2	Password	Enter the password required to login to the ISP	String, Alphanumeric username
3	Dial_number	Enter the number to dial to the ISP	String type

Sl No	Command Name	Description	Type and Description
4	AuthMethod	Setting Threeg authentication methods	Select from - NONE/PAP/CHAP
5	Apn	Enter the Apn Provided by the ISP	String
6	Reconnect_mode	Select Always On: The connection is always on OR On Demand :The connection will close after time specified in Idle_time field	Keepalive /idletimeout
7	Idle_time	The connection is automatically ended if it is idle for a specified number of minutes	Enter valid value from 5 to 999
8	Get_dns_from_isp	Enter Yes to get dns dynamically from ISP if you have not been assigned any static IP address	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
9	Primary_dns	Valid primary DNS Server IP Address	IP address, Primary dns
10	Secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
11	Cancel	Roll back wan configuration changes	
12	Exit	Save wan configuration changes and exit current mode	
13	Save	Save wan configuration changes	

8.35 net wan wan1-pppoeprofile add *prof_name*

Sl No	Command Name	Description	Type and Description
1	username	Enter the username to log in	String, Alphanumeric username
2	password	Enter the password to log in	String, Alphanumeric password
3	authOpt	Setting authentication options	Authentication option types like(Auto/PAP/CHAP/MS-CHAP/MS-CHAPv2)
4	connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
5	get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
6	primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
7	secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
8	get_ip_from_isp	Getting the ip mode type weather to get from ISP or static IP	Boolean Choice(Y/N)
9	static_ip	Setting static ip address if not obtaining the IP from ISP	IP address Static Ip

Sl No	Command Name	Description	Type and Description
10	subnet_mask	Setting Subnet Mask if not obtaining from ISP	IP address Subnet Mask
11	Service	Setting optional service name	String type
12	cancel	Roll back wan configuration changes	
13	exit	Save wan configuration changes and exit current mode	
14	save	Save wan configuration changes	

8.36 net wan wan2-pppoeprofile add *prof_name*

Sl No	Command Name	Description	Type and Description
1	username	Enter the username to log in	String, Alphanumeric username
2	password	Enter the password to log in	String, Alphanumeric password
3	authOpt	Setting authentication options	Authentication option types like(Auto/PAP/CHAP/MS-CHAP/MS-CHAPv2)
4	connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
5	get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
6	primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
7	secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
8	get_ip_from_isp	Getting the ip mode type weather to get from ISP or static IP	Boolean Choice(Y/N)
9	static_ip	Setting static ip address if not obtaining the IP from ISP	IP address Static Ip
10	subnet_mask	Setting Subnet Mask if not obtaining from ISP	IP address Subnet Mask
11	Service	Setting optional service name	String type
12	cancel	Roll back wan configuration changes	
13	exit	Save wan configuration changes and exit current mode	
14	save	Save wan configuration changes	

8.37 net wan wan1-pppoeprofile edit *prof_name*

Sl No	Command Name	Description	Type and Description
1	username	Enter the username to log in	String, Alphanumeric username
2	password	Enter the password to log in	String, Alphanumeric password
3	authOpt	Setting authentication options	Authentication option types like(Auto/PAP/CHAP/MS-CHAP/MS-CHAPv2)
4	connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
5	get_dns_from_isp	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses	Boolean Choice (Y/N), Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
6	primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
7	secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
8	get_ip_from_isp	Getting the ip mode type weather to get from ISP or static IP	Boolean Choice(Y/N)
9	static_ip	Setting static ip address if not obtaining the IP from ISP	IP address Static Ip
10	subnet_mask	Setting Subnet Mask if not obtaining from ISP	IP address Subnet Mask
11	Service	Setting optional service name	String type
12	cancel	Roll back wan configuration changes	
13	exit	Save wan configuration changes and exit current mode	
14	save	Save wan configuration changes	

8.38 net wan wan2-pppoeprofile edit *prof_name*

Sl No	Command Name	Description	Type and Description
1	username	Enter the username to log in	String, Alphanumeric username
2	password	Enter the password to log in	String, Alphanumeric password
3	authOpt	Setting authentication options	Authentication option types like(Auto/PAP/CHAP/MS-CHAP/MS-CHAPv2)
4	connectivity_type	Set connectivity type	ISP Connectivity Types. keepalive/idletimeout
5	get_dns_from_isp	Enter Yes to get dns dynamically from	Boolean Choice (Y/N),

Sl No	Command Name	Description	Type and Description
		ISP otherwise Enter No and give valid static dns addresses	Enter Yes to get dns dynamically from ISP otherwise Enter No and give valid static dns addresses
6	primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
7	secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
8	get_ip_from_isp	Getting the ip mode type weather to get from ISP or static IP	Boolean Choice(Y/N)
9	static_ip	Setting static ip address if not obtaining the IP from ISP	IP address Static Ip
10	subnet_mask	Setting Subnet Mask if not obtaining from ISP	IP address Subnet Mask
11	Service	Setting optional service name	String type
12	cancel	Roll back wan configuration changes	
13	exit	Save wan configuration changes and exit current mode	
14	save	Save wan configuration changes	

8.39 **net wan wan1-pppoeprofile delete** *prof_name*

Deletes wan1 pppoe profile

8.40 **net wan wan2-pppoeprofile delete** *prof_name*

Deletes wan2 pppoeprofile

8.41 net wan1 ipv6 configure

Sl No	Command Name	Description	Type and Description
1	Dhcpc stateless_mode_enable	Stateless mode configuration	stateless mode configuration. (StatelessAddrAutoConfig/Stateful AddrAutoConfig)
2	isp type	Set type of connection used static/dhcpc	Isp type, Static/dhcpc
3	Static gateway_address	Set ipv6 gateway address	IP Address Gateway address
4	static ip_address	set ipv6 address	IP Address, Static address

Sl No	Command Name	Description	Type and Description
5	static prefix	set prefix length	Integer, Prefix length
6	static primary_dns	Set ipv6 primary dns address	IP Address, Primary dns
7	static secondary_dns	Set ipv6 secondary dns address	IP Address, Secondary dns
8	Cancel	Roll back wan configuration changes	
9	Exit	Save wan configuration changes and exit current mode	
10	Save	Save wan configuration changes	

8.42 net wan wan2 ipv6 configure

Sl No	Command Name	Description	Type and Description
1	Dhcpc stateless_mode_enable	Stateless mode configuration	stateless mode configuration. (StatelessAddrAutoConfig/StatefulAddrAutoConfig)
2	Dhcpc prefix_delegation_enable	Prefix del egation configuration,	Boolean Choice(Y/N)
3	isp type	Set type of connection used static/dhcpc/PPPoE	Isp type, Static/dhcpc/PPPoE
4	Static gateway_address	Set ipv6 gateway address	IP Address Gateway address
5	static ip_address	set ipv6 address	IP Address, Static address
6	static prefix	set prefix length	Integer, Prefix length
7	static primary_dns	Set ipv6 primary dns address	IP Address, Primary dns
8	static secondary_dns	Set ipv6 secondary dns address	IP Address, Secondary dns
9	pppoe username	Enter the username to authenticate	String, Alphanumeric username
10	pppoe password	Enter the password to authenticate	String, Alphanumeric username
11	pppoe authOpt	Setting authentication options	Authentication option types like(Auto/PAP/CHAP/MS-CHAP/MS-CHAPv2)
12	pppoe dhcpv6_opt	Enter the dhcpv6 option for configuring additional parameters	Dhcpv6 options (Disable-Dhcpv6/Stateless-Dhcpv6/Stateful-Dhcpv6/Stateless-Dhcpv6-PrefixDelegation)

Sl No	Command Name	Description	Type and Description
13	pppoe primary_dns	Valid primary DNS Server IP Address	IP Address, Primary dns
14	pppoe secondary_dns	Valid secondary DNS Server IP Address	IP address, Secondary dns
15	Cancel	Roll back wan configuration changes	
16	Exit	Save wan configuration changes and exit current mode	
11	Save	Save wan configuration changes	

8.43 net routing protocol_binding add/edit

Sl No	Command Name	Description	Type and Description
1	destination_address_end	Ending IP of the Destination user	String
2	destination_address_start	Start IP of the Destination user	String
3	Destination_Network	Destination network type	ANY SINGLE_ADDRESS ADDRESS_RANGE
4	Local_Gateway	Local gateway type	Type: Dedicated WAN Configurable WAN
5	Service	Available Service	Default service types
6	source_address_end	Ending IP of the Source user	String IP address
8	source_address_start	Starting IP of the Source Network	String IP address
9	Source_Network	Source network type	ANY SINGLE_ADDRESS ADDRESS_RANGE
10	cancel .	Roll back configuration changes.	
11	Save	Save Protocol-Binding rules configuration changes	
12	show	Display system components' configuration	
13	Exit	Save routing protocol binding configuration and exit current mode	

8.44 routing protocol_binding enable <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row Id Of the rule to be enabled	Unsigned integer

8.45 routing protocol_binding edit

Sl No	Command Name	Description	Type and Description
1	row_id	Row Id Of the rule to be edited	Unsigned integer

8.46 routing protocol_binding disable

Sl No	Command Name	Description	Type and Description
1	row_id	Row Id Of the rule to be disabled	Unsigned integer

8.47 ddns wan2 configure DDNS configuration mode

Sl No	Command Name	Description	Type and Description
1	enable	Enable or disable Dyndns to provide Dynamic DNS service	Boolean Choice: Enable/Disable
2	hostname	Set Hostname	String
3	time_update_enable	Set Timeperiod as 30 days	Boolean Choice Y/N
4	Username	Set username	String Username
5	wild_flag_enable	Enable / Disable using wild cards.	Boolean Choice Enable/Disable
6	Password	Set password	String Password

8.48 dmz dhcp reserved_ip

Sl No	Command Name	Description	Type and Description
1	configure	DHCP Reserved IPs add/edit mode	String MAC Address
2	delete	Delete a specific reserved ip entry.	String MAC Address

Chapter 9. Configuration commands under branch SECURITY

9.1 security attack_checks configure

Sl No	Command Name	Description	Type and Description
1	echostorm_flood_rate <echostorm>	Configure the Echo Storm Flood Rate	Integer Configure Echo Storm Flood Rate (Value between 1-10000)
2	icmp_flood_rate <icmpflood>	Configure the ICMP flood Rate	Integer Configure ICMP Flood Rate (Value between 1-10000)
3	synflood_dectect_rate <synflood>	Configure the Syn flood Detect Rate	Integer Configure Syn Flood Detect Rate (Value between 1-10000)
4	respond_to_ping_enable <respondToPing>	Enable or Disable Respond To Ping on Internet Ports.	Enable / Disable Respond to Ping (Y/N)
5	stealth_mode_enable <stealthMode>	Enable or Disable Stealth Mode.	Enable / Disable Stealth Mode (Y/N)
6	tcp_block_enable <tcpBlock>	Enable or Disable TCP Flood on WAN port.	Enable / Disable TCP Flood on WAN (Y/N)
7	udp_block_enable <udpBlock>	Enable or Disable UDP Flood on LAN port.	Enable / Disable UDP Flood on LAN (Y/N)
8	cancel	Roll back Security Checks configuration changes.	
9	exit	Save Security Checks configuration changes and exit current mode.	
10	save	Save Security Checks configuration changes.	

9.2 security blocked_keywords add/edit

Sl No	Command Name	Description	Type and Description
1	group_name <group>	Keyword Blocking is applied to group name mentioned	String Group name
2	keyword <keyword>	Configure keyword to be blocked	String Keyword used for blocking traffic
3	cancel	Roll back blocked keywords configuration changes.	
4	exit	Save blocked keywords configuration changes and exit current mode.	
5	save	Save blocked keywords configuration changes.	

9.3 security blocked_keywords delete <row_id>

Sl No	Command Name	Description	Type and Description
1	security blocked_keywords delete <row_id>	Delete blocked keyword Rule	Row Id Of the rule to be deleted

9.4 security blocked_keywords disable <row_id>

Sl No	Command Name	Description	Type and Description
1	security blocked_keywords disable <row_id>	Disable blocked keyword Rule	Row Id Of the rule to be disabled

9.5 security blocked_keywords enable <row_id>

Sl No	Command Name	Description	Type and Description
1	security blocked_keywords enable <row_id>	Enable blocked keyword Rule	Row Id Of the rule to be enabled

9.6 security content_filtering configure

Sl No	Command Name	Description	Type and Description
1	enable <status>	Enable/Disable content Filtering	Enable/Disable content Filtering (Y/N)
2	activex_enable <activex>	enable/disable activex	enable/disable activex (Y/N)
3	cookies_enable <cookies>	enable/disable cookies	enable/disable cookies (Y/N)
4	java_enable <java>	enable/disable java	enable/disable java (Y/N)
5	proxy_enable <proxy>	enable/disable proxy	enable/disable proxy (Y/N)
6	cancel	Roll back content filtering configuration changes.	
7	exit	Save content filtering configuration changes and exit current mode.	
8	save	Save content filtering configuration changes.	

9.7 security custom_service add/edit

Sl No	Command Name	Description	Type and Description
1	destination_end_port	ending port number of the range used by destination user	Port of the Destination User (0..65535)
2	destination_start_port	Starting port number of the range used by destination user	Port of the Destination User (0..65535)

Sl No	Command Name	Description	Type and Description
3	name	Name of the service for which a rule is to be added	String, Service name
4	protocol	Protocol type	Protocol type (TCP/UDP/ICMP/ICMPv6)
5	quality_of_service	Type of QoS	QoS. (Normal-Service/Minimize-Cost/Maximize-Reliability/Maximize-Throughput/Minimize-Delay)
6	cancel	Roll back custom services configuration changes.	
7	exit	Save custom services configuration changes and exit current mode.	
8	save	Save custom services configuration changes.	

9.8 security custom_service delete <row_id>

Sl No	Command Name	Description	Type and Description
1	security custom_service delete <row_id>	Delete custom service row	Row Id Of the service to be deleted

9.9 security firewall ipv4 default_outbound_policy

Sl No	Command Name	Description	Type and Description
1	security firewall ipv4 default_outbound_policy_enable <default_outbound_policy>	Configure default outbound policy	enable/disable default ob policy (Y/N)

9.10 security firewall ipv4 configure/edit

Sl No	Command Name	Description	Type and Description
1	action <action>	Action to be taken by the rule	BLOCK_ALWAYS/ALLOW_ALWAYS/BLOCK_BY_SCHEDULE_ELSE_ALLOW/ALLOW_BY_SCHEDULE_ELSE _BLOCK, Type of Action to be taken by the rule
2	destination_address_end <dstAddrEnd>	End IP of the Destination user	IP Address End IP of the Destination User
3	destination_address_start <dstAddrStart>	Start IP of the Destination user	IP Address Start IP of the Destination user
4	destination_address_type <dstType>	Type of the destination user	Type of destination address, Any/Single Address/Address Range

Sl No	Command Name	Description	Type and Description
5	dnat_address <dnatAddr>	Send to Local Server (DNAT IP),Specifies an IP address and port number of a machine on the Local Network which is host	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	dnat_port <dnatport>	The port number to use for DNAT, required if port forwarding is enabled	Port number (0..65535)
7	log <log>	Enable / Disable Logs	Log type, Never/Always
8	schedule <schedule>	Schedule for which the rule is applicable	String Schedule for which the rule is applicable
9	service_name <service>	Name of the service for which a rule is to be added	String Name of the service for which a rule is to be added
10	snat_address <snatAddr>	IP of the SNAT Address	IP Address IP of the SNAT Address
11	snat_address_type <snatType>	Type of the SNAT address	snat type WAN1/Single Address
12	source_address_end <srcAddrEnd>	End IP of the Source user	IP Address End IP of the Source user
13	source_address_start <srcAddrStart>	Start IP of the Source user	Start IP of the Source user
14	source_address_type <srcType>	Type of the source user	Type of user address, Any/Single Address/Address Range
15	internet_destination <internetDest>	Enter WAN/OTHER. Set it as WAN port, if more than one is available, that is the internet destination for traffic covered by this firewall rule.	internet destination type (WAN/OTHERS)
16	internet_destination_address <internetDestAddr>	The WAN IP address that will map to the incoming server.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
17	port_forwarding_enable <dnatenable>	enable/disable port forwarding based on type of firewall rule configured	Boolean choice (Y/N)
18	rule_type <ruleType>	Type of rule to be configured	firewall rule type (WAN-To-LAN/Inbound/LAN-To-WAN/Outbound)
19	cancel	Roll back firewall ipv4 rules configuration changes	
20	exit	Save firewall ipv4 rules configuration changes and exit current mode.	
21	save	Save firewall ipv4 rules configuration changes.	

9.11 security firewall ipv4 delete <row_id>

Sl No	Command Name	Description	Type and Description
1	security firewall ipv4 delete	Row Id Of the rule to be deleted	Integer,

Sl No	Command Name	Description	Type and Description
	<row_id>		Row Id Of the rule to be deleted

9.12 security firewall ipv4 disable <row_id>

Sl No	Command Name	Description	Type and Description
1	security firewall ipv4 disable <row_id>	Row Id Of the rule to be disabled	Integer, Row Id Of the rule to be disabled

9.13 security firewall ipv4 enable

Sl No	Command Name	Description	Type and Description
1	security firewall ipv4 enable <row_id>	Row Id Of the rule to be enabled	Integer, Row Id Of the rule to be enabled

9.14 security ids configure

Sl No	Command Name	Description	Type and Description
1	enable <idsStatus>	Enable Intrusion detection system	Boolean choice (Y/N), Enable/Disable Intrusion detection system
2	intrusion_log_enable <intrusionLogStatus>	Enable/Disable intrusion logs	Boolean choice (Y/N), Enable/Disable intrusion logs
3	save	Save IDS configuration changes.	
4	exit	Save IDS configuration changes and exit current mode.	
5	cancel	Roll back IDS configuration changes.	

9.15 security ip_or_mac_binding add/edit

Sl No	Command Name	Description	Type and Description
1	ip_address <ipAddr>	configure ip address to which policies will be applied	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	log_dropped_packets <logStat>	Specify logging option for this rule	Boolean choice (Y/N), logging option for this rule
3	mac_address <macAddr>	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
4	name <name>	Specify a unique name for this rule.	name String
5	exit	Save ip mac binding configuration changes and exit current mode.	
6	save	Save ip mac binding configuration changes.	
7	cancel	Roll back ip mac binding configuration	

Sl No	Command Name	Description	Type and Description
		changes.	

9.16 security ip_or_mac_binding delete <row_id>

Sl No	Command Name	Description	Type and Description
1	security ip_or_mac_binding delete <row_id>	Row Id Of the rule to be deleted	Integer, Row Id Of the rule to be deleted

9.17 security port_triggering add/edit

Sl No	Command Name	Description	Type and Description
1	incoming_start_port <inPortStart>	start port number of the incoming traffic range	Port number, (0..65535)
2	incoming_end_port <inPortEnd>	end port number of the incoming traffic range	Port number, (0..65535)
3	name <name>	Name of the rule	String, Specifies an easily identifiable name for this rule
4	outgoing_start_port <outPortStart>	start port number of the outgoing traffic	Port number, (0..65535)
5	outgoing_end_port <outPortEnd>	end port of the outgoing traffic	Port number, (0..65535)
6	protocol <protocol>	Specify whether the port uses the TCP or UDP protocol	Protocol type, UDP/TCP
7	rule_enable <status>	specify whether to enable or disable the rule	Boolean choice (Y/N)
8	save	Save port triggering configuration changes.	
9	exit	Save port triggering rules configuration changes and exit current mode.	
10	cancel	Roll back port triggering configuration changes.	

9.18 security port_triggering delete <row_id>

Sl No	Command Name	Description	Type and Description
1	security port_triggering delete <row_id>	Row Id Of the rule to be deleted	Integer, Row Id Of the rule to be deleted

9.19 security schedules add/edit

Sl No	Command Name	Description	Type and Description
1	days all <allDays>	select all days for schedule	Boolean Choice (Y/N)
2	days monday <monday>	Select Monday for schedule	Boolean Choice (Y/N)
3	days tuesday <tuesday>	Select Tuesday for schedule	Boolean Choice (Y/N)
4	days wednesday <wednesday>	Select Wednesday for schedule	Boolean Choice (Y/N)
5	days thursday <thursday>	Select Thursday for schedule	Boolean Choice (Y/N)
6	days friday <friday>	Select Friday for schedule	Boolean Choice (Y/N)
7	days saturday <saturday>	Select Saturday for schedule	Boolean Choice (Y/N)
8	name <schedule>	Name of the schedule for which a rule can be added	String, Schedule name
9	time_of_day all_enable <allDay>	type of schedule activation for time of the day	Boolean Choice (Y/N)
10	time_of_day start hours <startSchedHours>	hours	schedule time unit type. (1..12)
11	time_of_day start mins <startSchedMins>	minutes	minute in the format MM(00-59)
12	time_of_day start meridiem <startSchedMeridian>	meridiem	Schedule Meridiem Type. (AM/PM)
13	time_of_day end hours <endSchedHours>	hours	schedule time unit type. (1..12)
14	time_of_day end mins <endSchedMins>	minutes	minute in the format MM(00-59)
15	time_of_day end meridiem <endSchedMeridian>	meridiem	Schedule Meridiem Type. (AM/PM)
16	cancel	Roll back schedules configuration changes	
17	save	Save schedules configuration changes.	
18	exit	Save schedules configuration changes and exit current mode.	

9.20 security schedules delete <row_id>

Sl No	Command Name	Description	Type and Description
1	security schedules delete <row_id>	Row Id Of the rule to be deleted	Integer, Row Id Of the rule to be deleted

9.21 security session_settings configure

Sl No	Command Name	Description	Type and Description
1	max_half_open_sessions <maxHalfOpenSess>	Maximum number of half open sessions configured	Integer, Max number of open sessions

Sl No	Command Name	Description	Type and Description
			configured
2	max_unidentified_sessions <maxUnIdentfdSess>	Maximum number of unidentified sessions	Integer, Max number of unidentified sessions
3	other_session_timeout <otherSessTimeout>	Configure other session timeout duration	Integer, Other Session Timeout Duration
4	tcp_session_cleanup_latency <tcpSessCleanupLatency>	Configure TCP session cleanup latency	Integer, TCP Session Cleanup Latency
5	tcp_session_timeout <tcpSessTimeout>	Configure TCP session timeout duration	Integer, TCP Session Timeout Durations
6	udp_session_timeout <udpSessTimeout>	Configure udp session timeout duration	Integer, UDP Session Timeout Duration
7	cancel	Roll back session settings configuration changes.	
8	save	Save security session settings configuration changes.	
9	exit	Save session settings configuration changes and exit current mode.	

9.22 security mac_filter source add/edit

Sl No	Command Name	Description	Type and Description
1	address <macAddr>	configure 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
2	cancel	Roll back source mac filter configuration changes.	
3	save	Save source mac filter configuration changes.	
4	exit	Save source mac filter configuration changes and exit current mode.	

9.23 security mac_filter source delete <row_id>

Sl No	Command Name	Description	Type and Description
1	security mac_filter source delete <row_id>	Row Id Of the rule to be deleted	Integer, Row Id Of the rule to be deleted

9.24 security mac_filter configure

Sl No	Command Name	Description	Type and Description
1	enable <status>	Enable/Disable the mac filter status	Boolean Choice (Y/N)
2	policy <policy>	Set the mac address policy	mac address policy type, Permit-And-Block-Rest/Block-And-Permit-Rest

Sl No	Command Name	Description	Type and Description
3	cancel	Roll back mac filter configuration changes.	
4	save	Save mac filter configuration changes.	
5	exit	Save mac filter configuration changes and exit current mode.	

9.25 security trusted_domain add/edit

Sl No	Command Name	Description	Type and Description
1	name <domain>	trusted domain name	String, Domain name
2	save	Save trusted domains configuration changes.	
3	exit	Save trusted domains configuration changes and exit current mode.	
4	cancel	Roll back trusted domains configuration changes.	

9.26 security trusted_domain delete

Sl No	Command Name	Description	Type and Description
1	security trusted_domain delete <row_id>	Row Id Of the rule to be deleted	Integer, Row Id Of the rule to be deleted

9.27 security vpn_passthrough configure

Sl No	Command Name	Description	Type and Description
1	ipsec_enable	Enable or Disable IPSEC Passthrough.	Enable / Disable IPSec Passthrough (Y/N)
2	l2tp_enable	Enable or Disable L2TP Passthrough.	Enable / Disable L2tp Passthrough (Y/N)
3	pptp_enable	Enable or Disable PPTP Passthrough.	Enable / Disable Pptp Passthrough (Y/N)
4	cancel	Roll back VPN Passthrough configuration changes	
5	exit	Save VPN Passthrough configuration changes and exit current mode.	
6	save	Save VPN Passthrough configuration changes	

9.28 security firewall ipv4 configure

Sl No	Command Name	Description	Type and Description
1	service_type	Name of the custom service or default	Choice

Sl No	Command Name	Description	Type and Description
		service for which a rule is to be added	NORMAL/CUSTOM
2	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 Custom service
3	service service_normal	Name of the service for which a rule is to be added	String Default service

Chapter 10. Configuration commands under branch SYSTEM

10.1 system logging facility configure <facility>

Sl No	Command Name	Description	Type and Description
1	system logging facility configure <facility>	Facility type to configure.	Facility types, Kernel/System/Local0-Wireless/Local1-UTM
2	level_options_set <level> <level_options> <enable>	Set level options. This command can be	Level identifier types, Emergency/Alert/Critical/Error/Warning/Notification/Information/Debugging Logging level options, Display_In_Event_Log/Send_to_syslog Enable, Enable/Disable this logging option. (Y/N)

10.2 system logging ipv4 configure

Sl No	Command Name	Description	Type and Description
1	bandwidth_limit_logs <bandwidthLimitLogs>	Bandwidth Limit logs Enable/Disable	Boolean Choice (Y/N)
2	broadcast_or_multicast_traffic_logs <broadcastOrMulticastTraffic>	All Broadcast/Multicast Traffic logs Enable/Disable	Boolean Choice (Y/N)
3	lan_wan_accept_packet_logs <acceptedPkts>	lan to wan accepted Pkts Enable/Disable	Boolean Choice (Y/N)
4	lan_wan_drop_packet_logs <droppedPkts>	lan to wan dropped Pkts Enable/Disable	Boolean Choice (Y/N)
5	source_mac_filter_logs <sourceMacFilter>	Source mac filter logs Enable/Disable	Boolean Choice (Y/N)
6	unicast_traffic_logs <unicastTrafficPkts>	All Unicast Traffic logs Enable/Disable	Boolean Choice (Y/N)
7	wan_lan_accept_packet_logs <acceptedPkts>	wan to lan accepted Pkts logs Enable/Disable	Boolean Choice (Y/N)
8	wan_lan_drop_packet_logs <droppedPkts>	wan to lan dropped Pkts logs Enable/Disable	Boolean Choice (Y/N)
9	cancel	Roll back logging configuration changes.	
10	save	Save logging configuration changes.	
11	exit	Save logging configuration changes and exit current mode.	

10.3 system logging remote configure

Sl No	Command Name	Description	Type and Description
1	email_logs_enable <enabled>	Set whether or not system emails scheduled	Email logs enabled or disabled. Boolean Choice (Y/N)
2	email_server <ip_address>	Set options for emailing of logs.	String, IP Address or internet name of an SMTP server.
3	identd_from_smtp_server_enable <identdSmtp>	Enable/Disable to identd from smtp server.	Enable/Disable identd from smtp server. Boolean Choice (Y/N)
4	log_identifier <identifier>	Set the log identifier prefixed to both,	String, Log identifier
5	return_email <email>	Set email address SMTP server replies are sent.	String, Return email address
6	schedule day <day>	Set schedule day.	Schedule day. Required only if unit is 'daily'. (Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday)
7	schedule meridiem <meridiem>	Set schedule meridiem.	Time in A.M. or P.M. Required only if unit is 'daily' or 'weekly'. (AM/PM)
8	schedule time <time>	Set schedule time.	Schedule time. Required only if unit is 'daily' or 'weekly'. (0:00/1:00/2:00/3:00/4:00/5:00/6:00/7:00/8:00/9:00 /10:00/11:00)
9	schedule unit <unit>	Set schedule unit.	Schedule unit. (Never/Hourly/Daily/Weekly)
10	send_to_email <email>	Set email address where logs and alerts will be sent.	String, Send to email address
11	smtp_auth password <password>	Set SMTP authentication password (for plain and CRAM-MD5 auth).	Password for SMTP authentication.
12	smtp_auth type <smtp_auth>	Set SMTP authentication types.	SMTP authentication types. (None/Plain/CRAM-MD5)
13	smtp_auth username <username>	Set SMTP authentication username (for plain and CRAM-MD5 auth).	Username for SMTP authentication.
14	syslog_server <serverName> facility severity	Set Syslog server.	String, Server name, syslog server address
15	Save	Save remoteLogging configuration changes.	
16	Exit	Save remote logging configuration changes and exit current mode.	
17	Cancel	Roll back remote logging configuration changes.	

10.4 system radius configure <radiusServer>

Sl No	Command Name	Description	Type and Description
1	server <ip_address>	Set RADIUS server IP address.	Radius server IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	authentication_port <port>	Set RADIUS server port.	RADIUS server port. (0..65535)
3	secret <secret>	Set RADIUS server secret.	RADIUS server secret string.
4	timeout <timeout>	Set RADIUS server connection timeout.	RADIUS server connection timeout (in seconds).
5	retries <retries>	Set RADIUS server connection retry attempts.	Integer, RADIUS server connection retry attempts.
6	cancel	Roll back configuration changes	
7	save	Save RADIUS configuration changes.	
8	exit	Save RADIUS configuration changes and exit current mode.	

10.5 system radius delete <radiusServer>

Sl No	Command Name	Description	Type and Description
1	radiusServer	IP address of RADIUS server to configure.	Radius server IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

10.6 system remote_management https configure

Sl No	Command Name	Description	Type and Description
1	enable <https_enable>	Enable/disable remote mgmt over https.	Enable/ Disable flag. (Y/N)
2	from_address <access_ip1>	Set the starting IP in case of range, and the IP to be allowed access in case of granting access to a particular machine	IP address.
3	end_address <access_ip2>	Set the Ending IP in case of range.	IP address
4	port <port>	Set the port you want to use for HTTP.	Integer, Port number
5	type <access_type>	Access type	0 -Enable access to all, 1 - Enable access to a range of IPs, 2 - Enable access to a single IP.
6	enable <https_enable>	Enable/disable remote mgmt over https.	Enable/ Disable flag. (Y/N)
7	save	save access Management changes for https.	

Sl No	Command Name	Description	Type and Description
8	exit	Save access Management changes for https and exit current mode.	
9	cancel	Roll back Remote Mgmt changes.	

10.7 system snmp sys configure

Sl No	Command Name	Description	Type and Description
1	contact <contact>	Set system contact information.	String, System contact identifier
2	location <location>	Set system location information.	String, System location identifier
3	name <name>	Set system name information.	String, System name identifier
4	cancel	Roll back snmp configuration changes.	
5	save	Save SNMP system configuration changes.	
6	exit	Save SNMP system configuration changes and exit current mode.	

10.8 system snmp trap configure <agentIp>

Sl No	Command Name	Description	Type and Description
1	agent <ip_address>	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	community <community>	The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community	String, Community name
3	port <port>	SNMP trap port the trap messages will be sent to.	Port number (0..65535)
4	subnet_mask <IPAddress>	The network mask used to determine the list of allowed SNMP managers. To allow any IP on the network to manager the dev	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	cancel	Roll back snmp configuration changes.	
6	exit	Save SNMP trap configuration changes and exit current mode.	
7	save	Save SNMP trap configuration changes.	

10.9 system snmp trap delete <agentIp>

Sl No	Command Name	Description	Type and Description
1	agentIp	The IP address of the SNMP agent.	IP address AAA.BBB.CCC.DDD

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

10.10 system snmp user configure

Sl No	Command Name	Description	Type and Description
1	authentication_algo	Choose between MD5 or SHA authentication	String MD5/SHA
2	authentication_password	Shared authentication password with the SNMPv3 user	String: Password
3	privacy_algorithm	DES-56 privacy is available for the authentication negotiation	String
4	privacy_password	shared privacy password with the SNMPv3 user	String
5	qos	[QoS configuration Mode]	String
6	Security	[Security configuration mode]	advanced_network: - Security advanced setup. application_rules: - Application Rules Configuration setup. Firewall: - Firewall rules setup. Ids: - IDS Configuration setup. ip_or_mac_binding - ip mac binding configuration mode. mac_filter - source mac filter configuration mode. schedules - Schedules Configuration setup. session_settings - Session Settings Configuration setup. website_filter - website filtering configuration setup.
7	security_level	authentication and privacy settings .	Security Level: NoAuth NoPriv Auth NoPriv AuthPriv
8	show	Display system components' configuration	
9	Cancel	Roll back SNMP v3 Users configuration changes.	
10	Save	Save SNMP trap configuration changes.	
11	exit	Save SNMP trap configuration	

Sl No	Command Name	Description	Type and Description
		changes and exit current mode.	

10.11 system time configure

Sl No	Command Name	Description	Type and Description
1	auto_daylight <auto_daylight>	Specify whether system automatically adjusts for daylight savings time	Boolean (Y/N) Specify whether system automatically adjusts for daylight savings time
2	ntp_server1 <ntp_server>	Set NTP server#1	String Server 1 Name / IP Address
3	ntp_server2 <ntp_server>	Set NTP server#2	String Server 2 Name / IP Address
4	timezone <tz>	Timezone	string Timezone (see note for values)
5	use_default_servers <enable>	Specify whether to use system default NTP servers	Boolean (Y/N) Enable/Disable use of default NTP servers
6	cancel	Roll back time configuration changes.	
7	exit	Save time configuration changes and exit current mode.	
8	save	Save time configuration changes.	

```
Note:
GMT :: Greenwich-Mean-Time-Edinburgh—London
GMT-12:00 :: Eniwetok-Kwajalein
GMT-11:00 :: Midway-Island-Samoa
GMT-10:00 :: Hawaii
GMT-09:30 :: Marqesas-Is.
GMT-09:00 :: Alaska
GMT-08:30 :: Pitciarn-Is.
GMT-08:00 :: Pacific-TimeCanada :: -Tijuana
GMT-08:00 :: Pacific-TimeUS :: Tijuana
GMT-07:00 :: Mountain-Time—ArizonaCanada
GMT-07:00 :: Mountain-Time—ArizonaUS
GMT-06:00 :: Mexico-CityUS—Canada
GMT-06:00 :: CentralTimeUSA
GMT-05:00 :: EasternTime
GMT-05:00 :: EasternTimeUSA :: Lima-Indiana-East
GMT-04:00 :: Atlantic-TimeCanada :: -Caracas
GMT-03:30 :: Newfoundland
GMT-03:00 :: Brasilia--Buenos-Aires
GMT-02:00 :: Mid-Atlantic
GMT-01:00 :: Azores--Cape-Verde-Is.
GMT+01:00 :: Europe
```

```
GMT+02:00 :: Athens--Istanbul--Minsk—Cairo
GMT+03:00 :: Baghdad--Kuwait—Moscow
GMT+03:30 :: Tehran
GMT+04:00 :: Abu-Dhabi--Muscat—Baku
GMT+04:30 :: Kabul
GMT+05:00 :: Ekaterinburg--Islamabad—Karachi
GMT+05:30 :: Bombay--Calcutta--Madras—Delhi
GMT+06:00 :: Almaty--Dhaka—Colombo
GMT+06:30 :: Burma
GMT+07:00 :: Bangkok--Hanoi—Jakarta
GMT+08:00 :: Beijing--Chongqing--Hong-Kong
GMT+09:00 :: Osaka--Sapporo--Tokyo--Seoul
GMT+09:30 :: Adelaide—Darwin
GMT+10:00 :: Brisbane--Guam--Port-Moresby
GMT+10:30 :: Lord-Howe-Is.
GMT+11:00 :: Magadan--Solomon-Is--New-Caledonia
GMT+11:30 :: Norfolk-I.
GMT+12:00 :: Auckland--Wellington--New-Zealand—Fiji
GMT+13:00 :: Tonga
GMT+14:00 :: Kiribati-Western-Samoa
```

10.12 system traffic_meter configure

Sl No	Command Name	Description	Type and Description
1	block_type <blockTraffic>	block_type <blockTraffic>	Traffic block types, Block-all-traffic/Block-all-traffic-except-email
2	counter <restartCounter>	set traffic counter as either specific time or restart counter now	Counter type, SpecificTime/RestartCounter
3	day_of_month <dayMonth>	set day of month	Calendar day of month (1..31)
4	increase_limit_by <incrLimitBy>	Set the value to increase limit of the traffic meter	Integer, Limit value
5	increase_limit_enable <incrLimitEnable>	Enable/Disable status of increase limit of the traffic meter option	Enable/disable limit option, Boolean choice (Y/N)
6	limit_type <trfLimitType>	Set traffic Limit Type	Traffic limit type, Nolimit/Downloadonly/BothDirections
7	monthly_limit <monthlyLimit>	Set the monthly limit value of the traffic meter	Integer, Monthly limit value
8	send_email_report <sendEmailReport>	Enable/Disable send email report	Enable/Disable send email report, Boolean Choice (Y/N)
9	send_email_alert <sendEmailAlert>	Enable/Disable send email alert	Enable/Disable send email alert, Boolean Choice (Y/N)
10	time_minute <timeMins>	set minutes for restart time	minute in the format MM(00-59)
11	time_hour <timeHrs>	set hours for restart time	HH(00-23) using 24 hour clock
12	cancel	Roll back traffic meter configuration changes.	

Sl No	Command Name	Description	Type and Description
13	save	Save traffic meter configuration changes.	
14	exit	Save traffic meter configuration changes and exit current mode.	

10.13 system group add

Sl No	Command Name	Description	Type and Description
1	groupname <groupname>	The name of the group	String
2	description <description>	A description of the group	String
3	capabilities <comma separatedl list of numeric codes>	A comma separated list of the numeric codes corresponding to the capabilities	String sslvpn user: 1, admin : 3 guest:4 xauth: 5, l2tp user: 7 pptp user: 8 captiveportal user: 10
4	grouptimeOut <timeout>	Time out for group	Integer

10.14 system group edit <row_id>

Sl No	Command Name	Description	Type and Description
1	system group edit <row id>	The rowid of the group to be edited	Integer

10.15 system group delete <row_id>

Sl No	Command Name	Description	Type and Description
1	system group delete <row id>	The rowid of the group to be deleted	Integer

10.16 system users add

Sl No	Command Name	Description	Type and Description
1	username <username>	Enter the username	String
2	FirstName <first_name>	The first name of the user (if any)	String
3	LastName <last_name>	The last name of the user (if any)	String
4	password <passwd>	The password for the user	String
5	password_confirm <passwd>	Re-enter the same password here	String
6	groupname <group_name>	Enter the group name to which this user belongs	String (The group should be created first)
7	usertimeout <timeout>	The timeout for this user	Integer

10.17 system users edit <row_id>

Sl No	Command Name	Description	Type and Description
1	system users edit <row id>	The rowid of the user to be edited	Integer

10.18 system users delete <row_id>

Sl No	Command Name	Description	Type and Description
1	system users delete <row id>	The rowid of the user to be deleted	Integer

10.19 system users password <user>

Sl No	Command Name	Description	Type and Description
1	system users password <user>	Password to be entered	String User to edit configuration

10.20 system usb usb1 configure

Sl No	Command Name	Description	Type and Description
1	printer_enable	Enable printer usb	To enable printer for USB 1
2	Storage_enable	Enable Storage USB	To enable storage for USB 1

10.21 system usb usb2 configure

Sl No	Command Name	Description	Type and Description
1	printer_enable	Enable printer usb	To enable printer for USB 2
2	Storage_enable	Enable Storage USB	To enable storage for USB 2

Chapter 11. Configuration commands under branch DOT11

11.1 dot11 access point configure <ap_name>

Sl No	Command Name	Description	Type and Description
1	ap_name	Unique name of the access point	String, Access point name
2	acl_policy_status	Policy, Set the default ACL policy for AP.	policy Name of the policy. (Open/Allow/Deny)
3	enable_active_time	Indicates if the AP is enabled/disabled by a daily timer.	indicates if the AP is enabled/disabled by a daily timer. (Y/N)
4	max_associated_clients	Set maximum number of client that can associate with AP.	Maximum number of clients.
5	start_time hour	the hour of the day when the AP is activated (and available for use if enabled).	Hours 1 to 12
6	start_time meridian	the meridian of the day when the AP is activated (and available for use if enabled).	Meridiem am/pm
7	start_time minute	the minute of the day when the AP is activated (and available for use if enabled).	Minute in the format MM (00-59)
8	stop_time hour	the hour of the day when the AP is deactivated.	Hours 1 to 12
9	stop_time meridian	the meridian of the day when the AP is deactivated	Meridiem am/pm
10	stop_time minute	the minute of the day when the AP is deactivated	Minute in the format MM (00-59)
11	cancel	Roll back AP configuration changes	
12	exit	Save AP configuration changes and exit current mode.	
13	save	Save AP configuration changes	

11.2 dot11 access point delete <ap_name>

Sl No	Command Name	Description	Type and Description
1	ap_name	Unique name of the access point	String, Access point name

11.3 dot11 access point disable <ap_name>

Sl No	Command Name	Description	Type and Description
1	ap_name	Unique name of the access point	String, Access point name

11.4 dot11 access point enable <ap_name>

Sl No	Command Name	Description	Type and Description
1	ap_name	Unique name of the access point	String, Access point name

11.5 dot11 access point mac add <ap_name> <mac_address>

Sl No	Command Name	Description	Type and Description
1	ap_name	Unique name of the access point	String, Access point name
2	mac_address	MAC address to add to ACL	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

11.6 dot11 access point mac delete <ap_name> <mac_address>

Sl No	Command Name	Description	Type and Description
1	ap_name	Unique name of the access point	String, Access point name
2	mac_address	MAC address to delete to ACL	MAC address AA:BB:CC:DD:EE:FF where each part is in the range 00-FF

11.7 dot11 profile configure <profile_name>

Sl No	Command Name	Description	Type and Description
1	profile_name	Unique name of the profile	String, profile name
2	advanced 8021X_re_authentication_interval	Set advanced profile re authentication interval options.	802.1X Re-authentication Interval (in seconds). [10]
3	advanced association_timeout	Set advanced profile association timeout options.	Association timeout (in seconds). [10]
4	advanced authentication_timeout	Set advanced profile authentication timeout options.	Authentication timeout (in seconds). [10]
5	advanced	Set advanced profile group key refresh	Group Key refresh interval (in

Sl No	Command Name	Description	Type and Description
	group_key_refresh_interval	interval options.	seconds). [10]
6	advanced pmksa_lifetime	Set advanced profile pmksa lifetime options.	PMKSA Lifetime (in seconds). [10]
7	broadcast_ssid	Enable or disable SSID broadcast.	Enable or disable. (Y/N)
8	default_cos	Set default Class Of Service	Default QoS. (Background/BestEffort/Video/Voice)
9	qos_enable	Enable or disable QoS	QoS enable or disable. (Y/N)
10	ssid	Set the 802.11 profile SSID.	Ssid name
11	wep authentication	Set WEP authentication type.	WEP authentication type. (Automatic/Open-System/Shared-Key)
12	wep encryption	Set WEP encryption type.	WEP encryption type. (64-bit-WEP/128-bit-WEP/152-bit-WEP)
13	wep key <index> <key>	Set WEP key. Not required if passphrase is set.	Index, Index at which key is installed. (1/2/3/4) key WEP Key.
14	wep passphrase <index> <passphrase>	Set WEP passphrase to generate WEP key from.	Index, Index at which key is installed. (1/2/3/4) passphrase to use to generate WEP Key.
15	wpa authentication	Set WPA authentication type.	WPA authentication type. (PSK/RADIUS/PSK+RADIUS)
16	wpa encryption	Set WPA encryption type.	WPA encryption type. (TKIP/CCMP/TKIP+CCMP)
17	wpa password	WPA Password. Needed only if authentication is PSK	String, WPA Password
18	exit	Save profile configuration changes and exit current mode.	
19	save	Save profile configuration changes	

11.8 dot11 radio advanced configure <radio_num>

Sl No	Command Name	Description	Type and Description
1	radio_num	Radio to configure	Unsigned integer, Radio number
2	beacon_interval <interval>	Set the time between beacon transmissions (in milliseconds).	Time between beacon transmissions (in milliseconds)
3	dtim_interval <interval>	Set the interval between delivery traffic indication message.	Delivery traffic indication message interval (in milliseconds).
4	fragmentation_threshold <threshold>	Set the maximum length of the frame.	Maximum length of the frame.
5	long_retry_limit <limit>	Set the retry limit for frame retransmission on transmission failure.	Frame re-transmission limit.

Sl No	Command Name	Description	Type and Description
6	preamble_mode <preamble>	Set the 802.11b preamble type to be prepended to every frame	802.11b preamble type to be prepended to every frame (Long/Short)
7	rts_cts_protection <enabled>	Enable/disable RTS/CTS handshake before packet transmission.	Enable/Disable RTS/CTS handshake. (Y/N)
8	rts_threshold <threshold>	Set the Request to Send (RTS) threshold.	Request to Send (RTS) threshold.
9	short_retry_limit <limit>	Set the retry limit for frame retransmission on transmission failure.	Frame re-transmission limit.
10	cancel	Roll back radio configuration changes	
11	exit	Save radio configuration changes and exit current mode.	
12	save	Save radio configuration changes	

11.9 dot11 radio configure <radio_num>

Sl No	Command Name	Description	Type and Description
1	radio_num	Radio to configure	Unsigned integer, Radio number
2	channel <channel>	Set the channel used by radio.	Unsigned integer, Channel number (or Auto to let system select).
3	channel_spacing <value>	Select either 20 MHz or 40 MHz channel bonding (spacing).	Select either 20 MHz or 40 MHz channel bonding (spacing) (20MHz/20-40MHz/40MHz)
4	country <country>	Set country.	country name (USA/INDIA/CANADA/HONG_KONG/CHINA/AUSTRALIA/SINGAPORE/THAILAND/BRUNEI_DARUSSALAM/INDONESIA/NEW_ZEALAND/PHILIPPINES/VIETNAM)
5	default_transmit_power <value>	Set default trans power for APs using this radio.	Transmitted power level (in %) (100%/75%/50%/25%/0%)
6	operating_frequency <value>	Select either 2.4GHz or 5GHz based on the radio's capabilities and your wireless network requirements.	Select either 2.4GHz or 5GHz based on the radio's capabilities and your wireless network requirements (2.4GHz/5GHz)
7	cancel	Roll back radio configuration changes	
8	exit	Save radio configuration changes and exit current mode.	
9	save	Save radio configuration changes	

Chapter 12. Configuration commands under branch VPN

12.1 vpn ipsec policy connect <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	rowid of vpn policy to connect and establish an inactive SA (connection).	Unsigned integer, row_id of vpn policy

12.2 vpn ipsec policy drop <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	rowid of vpn policy to disconnect and terminate an active SA (connection)	Unsigned integer, row_id of vpn policy

12.3 vpn ipsec policy delete <name>

Sl No	Command Name	Description	Type and Description
1	Name	Unique ike policy name	String, Ike policy name

12.4 vpn ipsec policy configure <name>

Sl No	Command Name	Description	Type and Description
1	name	Unique vpn policy name	String, vpn policy name
2	general_policy_type	For manual policy All settings (including the keys) for the VPN tunnel are manually input for each end point. No third-party server or organization is involved. **for auto policy** Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN Endpoi	Vpn PolicyType(Manual Policy/ Auto Policy)
3	general_ike_version	Select the ike version	Vpn ikeversion(IKEV1 /IKEV2)
4	general_ipsec_mode	This can be either 'Tunnel' mode or 'Transport' modeTransmode is used when we want to secure communication only between two gateways	IPSecMode(Tunnel /Transport)

Sl No	Command Name	Description	Type and Description
5	general_select_local_gateway	In the event two WAN ports are configured to connect to an ISP, select the gateway that will be used as the local endpoint for this IPsec tunnel.	Vpn Local gateway (DedicatedWAN/ConfiguredWAN)
6	general_remote_end_point_type	Select the type of identifier that you want to provide for the gateway at the remote endpoint: IP Address or FQDN (Fully Qualified Domain Name)	Remote end point type(Ipadress /fqdn)
7	general_remote_end_point ipaddress	IPAdress of the remote host	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255,remote end pointt
8	general_remote_end_point fqdn	Full Qualified Domain Name of remote host	String,remote end point
9	general_enable_mode_config	Enables Mode Config feature. Mode Config is similar to DHCP and is used to assign IP addresses to remote VPN clients, like iPhone VPN Client.	ModeConfig Boolean choice (Y/N)
10	general_enable_netbios	enable/disable this to allow NetBIOS broadcasts to travel over the VPN tunnel.	netbiosenable Boolean choice (Y/N)
11	general_enable_rollover	Check this box to allow the VPN to rollover when WAN Mode is set to Auto Rollover on the WAN Mode page.	RollOver Boolean choice (Y/N)
12	general_protocol	Select protocol of the tunnel	Vpn Protocol (AH/ESP)
13	general_enable_dhcp	Check this box to allow VPN clients to connect to your router over IPsec and get an assigned IP using DHCP.	DHCP over ipsec Boolean (Y/N)
14	general_local_network_type	Select the IP addresses on the local side that will be part of the tunnel. This can be either a single IP address, several IP addresses in a range, an entire subnet, or any IP address that want to connect.	vpn network type (ANY/SINGLE/RANGE/SUBNET)
15	general_local_start_address	IP address from where the range needs to begin	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
16	general_local_end_address	IP address where the range needs to end	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
17	general_local_subnet_mask	Subnet mask of the subnet used	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
18	general_remote_network_type	Select the IP addresses on the remote side that will be part of the tunnel. This can be either a single IP address, several IP addresses in a range, an	vpn network type (ANY/SINGLE/RANGE/SUBNET

Sl No	Command Name	Description	Type and Description
		entire subnet, or any IP address that wants to connect.	
19	general_remote_start_address	IP address from where the range needs to begin	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
20	general_remote_end_address	IP address where the range needs to end	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
21	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
22	auto_phase1_exchange_mode	Main mode negotiates the tunnel with higher security, but is slower whereas Aggressive mode establishes a faster connection.	Exchange mode type, (Main/Aggressive)
23	auto_phase1_direction_type	The connection methods for this router can be one of the selected	Direction type, (Initiator/Responder/Both)
24	auto_phase1_enable_nat_traversal	Set NAT traversal to 'On' if you expect any Network Address Translation (NAT) to occur during IPsec communication. If not set this option to Off.	Nat Traversal Boolean Choice (Y/N)
25	auto_phase1_nat_keepalive_frequecy	When NAT traversal is set to 'On', use this option to control the keep-alive-frequency value. Keep-alive packets are sent at the mentioned time interval and these are used to keep the NAT mappings alive on the NAT device. Setting this value to 0 disables this feature.	Unsigned integer
26	auto_phase1_local_identtype	The ISAKMP identifier for this router	The ISAKMP identifier for this router (IP/FQDN/User FQDN/DER ASN1 DN) (Local-Wan-IP/FQDN/User-FQDN/DE R-ASN1-DN)
27	auto_phase1_local_identifier	The value of the respective option chosen in the Identifier Type	The value of the respective option chosen in the Identifier Type
28	auto_phase1_remote_identtype	The ISAKMP identifier for the remote device	The ISAKMP identifier for the remote device. (IP/FQDN/User FQDN/DER ASN1 DN) (Local-Wan-IP/FQDN/User -FQDN/DER-ASN1-DN)
29	auto_phase1_remote_identifier	The value of the respective option chosen in the Identifier Type	The value of the respective option chosen in the Identifier Type
30	auto_phase1_encryption_algorithm	The algorithm used to negotiate the SA. There are four algorithms supported by this router: DES, 3DES, AES-128, AES-192.AES-256/BLOWFISH/CAST128	(None/DES/3DES/AES-128/AES-192/AES-256 /BLOWFISH/CAST128)

Sl No	Command Name	Description	Type and Description
31	auto_phase1_key_length	BLOWFISH and CAST128 are variable length algorithms, and so the key length field is required when using either of these encryption types. For BLOWFISH, the Key Length must be between 40 and 448 and it must be a multiple of 8. For CAST128, the Key Length must be between 40 and 128 and it must be a multiple of 8	Unsigned integer
32	auto_phase1_auth_algorithm	Specify the authentication algorithm for the VPN header. There are many algorithms	Specify the authentication algorithm for the VPN header. Algorithms supported by this router: MD5/SHA-1/SHA2-256/SHA2-384/SHA2-512)
33	auto_phase1_auth_method	Select Pre-shared key for a simple password based key. Selecting RSA-Signature will disable the pre-shared key text box and uses the Active Self Certificate uploaded in the Certificates page. In that case, a certificate must be configureD	Pre-shared key/RSA Signature (Pre-shared-Key/RSA-Signature)
34	auto_phase1_pre_shared_key	alpha-numeric key to be shared with IKE peer	String, alpha-numeric key to be shared with IKE peer
35	auto_phase1_dh_group	The Diffie-Hellman algorithm is used when exchanging keys. The DH Group sets the strength of the algorithm in bits.	(None/Group1/Group2/Group5/Group14/Group15/Group16/Group17/Group18)
36	auto_phase1_sa_lifetime	the interval after which the Security Association becomes invalid.	Unsigned integer,
37	auto_phase1_enable_dead_peer_detection	Dead Peer Detection is used to detect whether the Peer is alive or not. If peer is detected as Dead, it deletes the IPs	Boolean (Y/N)
38	auto_phase1_detection_period	Detection Period is the interval between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when	Unsigned integer, Detection period interval
39	auto_phase1_reconnect_failure_count	Maximum number of DPD failures allowed before tearing down the connection.	Unsigned integer, Dpd failure count
40	auto_phase1_extended_authentication	Rather than configuring a unique VPN policy for each user, you can enable the VPN gateway router to authenticate users from a stored list of user accounts or with an external authentication server such as a RADIUS server. When connecting many VPN clients to a VPN gateway router, XAUTH allows authentication of users with methods in addition to the	Extebded Authentication (NONE/IPSec Host/Edge Device)

Sl No	Command Name	Description	Type and Description
		authentication method mentioned in the IKE SA parameters.	
41	auto_phase1_authentication_type	If userdata base is selected authentication done using local Database.If Radius option is selected authentication is done using external radius server	Authentication type (User DataBase / Radius-PAP / Radius-CHAP)
42	auto_phase1_xauth_password	The password can contain alphanumeric characters	String, The password can contain alphanumeric characters
43	auto_phase1_xauth_username	This is the unique identifier for the user, and can contain any alphanumeric characters	This is the unique identifier for the user, and can contain any alphanumeric characters.
44	manual_spi_in	Takes a hexadecimal value between 3 and 8 characters	spiin Unsigned integer
45	manual_spi_out	Takes a hexadecimal value between 3 and 8 characters	Spiiout Unsigned integer
46	manual_encryption_algorithm	The algorithm used to encrypt the data	vpn encryption algorithm (None/DES/3DES/AES-128/AES-192/AES-256/AES-CCM/AES-GCM//TWOFISH(128/192/256)/ BLOWFISH/CAST128)
47	manual_key_length	BLOWFISH and CAST128 are variable length algorithms, and so the key length field is required when using either of these encryption types. For BLOWFISH, the Key Length must be between 40 and 448 and it must be a multiple of 8. For CAST128, the Key Length must be between 40 and 128 and it must be a multiple of 8.	Unsigned integer
48	manual_encryption_key_in	Encryption key of the inbound policy. The length of the key depends on the algorithm chosen	String
49	manual_encryption_key_out	cryption key of the outbound policy. The length of the key depends on the algorithm chosen.	String
50	manual_authentication_algorithm	Algorithm used to verify the integrity of the data.	vpn authentication algorithm (MD5/SHA-1/SHA2-256/SHA2-384/SHA2-512)
51	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
52	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
53	auto_phase2_sa_	It is the interval after which the Security Association becomes invalid	salifetime Unsigned integer

Sl No	Command Name	Description	Type and Description
	lifetime		
54	auto_phase2_encryption_algorithm	The algorithm used to encrypt the data	vpn encryption algorithm (None/DES/3DES/AES-128/AES-192/AES-256/AES-CCM/AES-GCM//TWOFISH(128/192/256)/ BLOWFISH/CAST128)
55	auto_phase2_key_length	BLOWFISH and CAST128 are variable length algorithms, and so the key length field is required when using either of these encryption types. For BLOWFISH, the Key Length must be between 40 and 448 and it must be a multiple of 8. For CAST128, the Key Length must be between 40 and 128 and it must be a multiple of 8.	Unsigned integer
56	auto_phase2_authentication_algorithm	Algorithm used to verify the integrity of the data.	vpn authentication algorithm (MD5/SHA-1/SHA2-256/SHA2-384/SHA2-512)
57	auto_phase2_enable_pfskeygroup	Enable Perfect Forward Secrecy (PFS) to improve security. While slower, this protocol helps to prevent eavesdroppers by ensuring that a Diffie-Hellman exchange is performed for every phase-2 negotiation.	PFSKeyGroup enable Boolean (Y/N)
58	auto_phase2_dh_group	The Diffie-Hellman algorithm is used when exchanging keys. The DH Group sets the strength of the algorithm in bits.	vpn Diffie-Hellman (DH) Groups (None/Group1/Group2/Group5 Group14/Group15/Group16/Group 17/Group18)
59	save	Save vpn policy configuration changes.	
60	cancel	Roll back vpn policy configuration changes.	
61	exit	Save vpn policy configuration changes and exit current mode.	

12.5 vpn ipsec policy disable <name>

Sl No	Command Name	Description	Type and Description
1	name	Name of vpn policy to be disabled	Unsigned integer, Policy name

12.6 vpn ipsec policy enable <name>

Sl No	Command Name	Description	Type and Description
1	name	Name of vpn policy to be enabled	Unsigned integer, Policy name

12.7 vpn ipsec dhcp configure

Sl No	Command Name	Description	Type and Description
1	Start_address	The starting IP address of the range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	End_address	The end IP address of the range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
3	Subnet_mask	Subnet Mask for the mentioned range.	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12.8 vpn sslvpn client

Sl No	Command Name	Description	Type and Description
1	enable_fulltunnel	Yes for full tunnel, No for split tunnel	Boolean (Y/N)
2	dns_suffix	DNS Suffix	String
3	primary_dns	Primary DNS Server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
4	secondary_dns	Secondary DNS Server	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	begin_clientaddress	Client address range begin	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	end_clientaddress	Client address range end	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	lcp_timeout	LCP Timeout	Unsigned integer

12.9 vpn sslvpn policy add/edit

Sl No	Command Name	Description	Type and Description
1	policy_type	Policy For	Global, group, user
2	policy_owner	Polcy owner	Global if global policy, group name if group policy and user name if user policy
3	destination_objecttype	Apply Policy to	Netowrk-Resource, IP-Address, IP-Network, All-Addresses
4	policy_name	Policy Name	String, Max 128 characters and no ‘ or empty space or “
5	policy_address	Policy IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-

Sl No	Command Name	Description	Type and Description
			255
6	policy_masklength	Mask Length	number in range of 0 to 32
7	start_port	Begin port	Port number
8	end_port	End port	Port number
9	service_type	Defined service	VIRTUAL-PASSAGE, VIRTUAL-TRANSPORT, all(all)
10	resource_name	Defined Resource	String, Max 128 characters and no ‘ or empty space or “
11	policy_permission	Permission	Permit, Deny
12	icmp_block	Block Icmp	Boolean (Y/N)

12.10 vpn sslvpn policy delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of policy to be deleted	Unsigned integer, Row number

12.11 vpn sslvpn portal-layouts add/edit

Sl No	Command Name	Description	Type and Description
1	portal_name	Portal Layout Name	String, Max 128 characters and no ‘ or empty space or “
2	portal_title	Portal Site Title	String, Max 128 characters and no ‘ or empty space or “
3	banner_title	Banner Title	String, Max 128 characters and no ‘ or empty space or “
4	banner_message	Banner Message	String, no ‘ or empty space or “
5	display_banner	Display Banner Message on login page	Boolean (Y/N)
6	enable_httpmetatags	HTTP Meta tags for cache control	Boolean (Y/N)
7	enable_activexwebcachecleaner	ActiveX webcache cleaner	Boolean (Y/N)
8	enable_vpntunnel	VPN Tunnel Page	Boolean (Y/N)
9	enable_portforwarding	Port Forwarding	Boolean (Y/N)

12.12 vpn sslvpn portal-layouts delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of portal layout to be deleted	Unsigned integer, Row number

12.13 vpn sslvpn portforwarding appconfig add

Sl No	Command Name	Description	Type and Description
1	serverip	Local Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	port	TCP Port Number	Port Number

12.14 vpn sslvpn portforwarding appconfig delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of application configuration rule to be deleted	Unsigned integer, Row number

12.15 vpn sslvpn portforwarding hostconfig add

Sl No	Command Name	Description	Type and Description
1	serverip	Local Server IP Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	domain_name	Fully Qualified Domain Name	String, Max 128 characters and no ‘ or empty space or “

12.16 vpn sslvpn portforwarding hostconfig delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of host configuration rule to be deleted	Unsigned integer, Row number

12.17 vpn sslvpn resource add

Sl No	Command Name	Description	Type and Description
1	resource_name	Resource Name	String, Max 128 characters and no ‘ or empty space or “
2	service_type	Service	VIRTUAL-PASSAGE, VIRTUAL-TRANSPORT, all(all)

12.18 vpn sslvpn resource delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of resource to be deleted	Unsigned integer, Row number

12.19 vpn sslvpn resource configure add <resource_name>

Sl No	Command Name	Description	Type and Description
1	resource_name	Resource name	String, Max 128 characters and no ‘ or empty space or “
2	object_type	Object Type	IP-Address, IP-Network
3	object_address	Object Address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
4	mask_length	Mask Length	number in range of 0 to 32
5	start_port	Begin port number	Port number
6	end_port	End port number	Port number
7	icmp_block	Block Icmp	Boolean (Y/N)

12.20 vpn sslvpn resource configure delete <row_id> <resource_name>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of resource object to be deleted	Unsigned integer, Row number
2	Resource_name	Resource name	String, Max 128 characters and no ‘ or empty space or “

12.21 vpn sslvpn route add

Sl No	Command Name	Description	Type and Description
1	destination_network	Destination Network	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
2	subnet_mask	Subnet Mask	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

12.22 vpn sslvpn route delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of route to be deleted	Unsigned integer, Row number

12.23 vpn sslvpn users domains add

Sl No	Command Name	Description	Type and Description
1	domain_name	Domain Name	String of any character type with no spaces
2	authentication_type	Authentication type for the domain	Local user database,Radius PAP,Radius Chap,Radius MSCHAP,Radius MSCHAPV2,NT Domain,Active Directory and LDAP
3	portal	Portal to which the domain belongs	String of any character type with no spaces
4	authentication_server1	First Authentication server address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	g authentication_server2	Second Authentication server address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	authentication_server3	Third Authentication server address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	timeout	Timeout for the authentication	Positive Integer range
8	retries	Retries to the server	Positive Integer range
9	authentication_secret	Secret key to the authentication server	String of any character type with no spaces
10	authentication_secret2	Secondary secret key to the authentication server	String of any character type with no spaces
11	workgroup	Workgroup	String of any character type with no spaces
12	Second_workgroup	Secondary work group	String of any character type with no spaces
13	ldap_base_dn	Ldap base domain name	String of any character type with no spaces
14	second_ldap_base_dn	Secondary Ldap base domain name	String of any character type with no spaces

Sl No	Command Name	Description	Type and Description
15	active_directory_domain	Active directory domain	String of any character type with no spaces
17	second_active_directory_domain	Secondary Active directory domain	String of any character type with no spaces

12.24 vpn sslvpn users domains edit <domainname>

Sl No	Command Name	Description	Type and Description
1	domain_name	Domain Name	String of any character type with no spaces
2	authentication_type	Authentication type for the domain	Local user database,Radius PAP,Radius Chap,Radius MSCHAP,Radius MSCHAPV2,NT Domain,Active Directory and LDAP
3	portal	Portal to which the domain belongs	String of any character type with no spaces
4	authentication_server1	First Authentication server address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
5	g authentication_server2	Second Authentication server address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
6	authentication_server3	Third Authentication server address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
7	timeout	Timeout for the authentication	Positive Integer range
8	retries	Retries to the server	Positive Integer range
9	authentication_secret	Secret key to the authentication server	String of any character type with no spaces
10	authentication_secret2	Secondary secret key to the authentication server	String of any character type with no spaces
11	workgroup	Workgroup	String of any character type with no spaces
12	Second_workgroup	Secondary work group	String of any character type with no spaces
13	ldap_base_dn	Ldap base domain name	String of any character type with no spaces

Sl No	Command Name	Description	Type and Description
14	second_ldap_base_dn	Secondary Ldap base domain name	String of any character type with no spaces
15	active_directory_domain	Active directory domain	String of any character type with no spaces
17	second_active_directory_domain	Secondary Active directory domain	String of any character type with no spaces

12.25 vpn sslvpn users domains delete <domainname>

Sl No	Command Name	Description	Type and Description
1	domainname	Row id of domain to be deleted	Unsigned integer, Row number

12.26 vpn sslvpn users users login_policies <user_row_id>

Sl No	Command Name	Description	Type and Description
1	disable_login	Deny the user to login	Boolean (Y/N)
2	deny_login_from_wan_interface	Deny the user from Wan interface	Boolean (Y/N)

12.27 vpn sslvpn users users ip_policies configure <user_row_id>

Sl No	Command Name	Description	Type and Description
1	allow_login_from_defined_addresses	Allow login	Boolean (Y/N)
2	add_ip_address	Add Ip Address	Boolean (Y/N)
3	source_address_type	Source Address Type	Ip address or Ip netwok
4	source_address	Source ip address	IP address AAA.BBB.CCC.DDD where each part is in the range 0-255

Sl No	Command Name	Description	Type and Description
5	mask_length	Source network mask length	Integer range 1 to 32

12.28 vpn sslvpn users users ip_policies delete <row_id>

Sl No	Command Name	Description	Type and Description
1	row_id	Row id of policy table to be deleted	Unsigned integer, Row number

12.29 vpn sslvpn users users browser_policies <user_row_id>

Sl No	Command Name	Description	Type and Description
1	allow_login_from_defined_browsers	Allow the user to login from defined browser	Boolean (Y/N)
2	add defined browser	Add the defined browser	Boolean (Y/N)
3	client_browser	Select the browser	Internet explorer,Mozilla,Firefox,Netscape,opera
4	del_client_browser	Delete the browser	Boolean (Y/N)