FlexDSL Telecommunications AG

FlexDSL GigaFlex

DIN-RAIL UNITS

CONFIGURATION MANUAL

Version:	1.1
Document name:	UM_FlexDSL-GigaFlex_Software_v1-1.docx
Revision:	16 October 2019

VERSION CONTROL

Manual Version	Date	Software Version	Major changes to previous version
1.0	26.02.2019	1.0.12	Initial Version
1.1	08.10.2019	1.0.40	Chapter 1 “Precaution” corrected New Chapter 4.5 ”Alarm Configuration” Chapter 5.2 “License” corrected Chapter 7.2.1 “The Bonding Groups and Port Association” corrected. Chapter 7.2.2. New parameter “multipair” for the DSL-Bonding Group command. New alias: SHDSL-Bonding Group New parameter “auto” for the Master command, chapter 7.2.7 Chapter 7.2.9 “Threshold” corrected New command Set Baserate PAM Extended, chapter 7.2.11 New chapter 8.1 “Authentication Methods” Chapter 8.2.1 ”Username” corrected New command Set Minimum Password Length, chapter 8.2.2 New chapter 8.4 ”Authentication with TACACS” Chapter 14 “SNMP Configuration” optimised.

SAFETY REGULATIONS

IF THE UNIT IS NOT USED IN ACCORDANCE TO REGULATIONS DESCRIBED AND DEFINED IN THE CHAPTERS ”TECHNICAL DESCRIPTION” AND “TECHNICAL SPECIFICATIONS”, FLEXDSL TELECOMMUNICATIONS AG REFUSES TO TAKE ANY RESPONSIBILITY. FURTHERMORE, NO WARRANTY IS GRANTED IN SUCH CASE!

IT’S ONLY ALLOWED TO USE EXTERNAL POWER SUPPLYS THAT ARE APPROVED ACCORDING TO THE SAFETY STANDARD IEC/EN 60950-1.

IT’S ONLY ALLOWED TO USE THE UNITS WITH HOUSINGS SUPPLYED FROM FLEXDSL TELECOMMUNICATIONS AG (SUBRACKS, MINIRACK, UTTX). THE RACK MUST BE CONNECTED PERMANENTLY TO RELIABLE PROTECTIVE EARTH CONDUCTOR. THE NTU UNIT MUST BE CONNECTED PERMANENTLY TO RELIABLE PROTECTIVE EARTH CONDUCTOR: THE LTU UNIT HAS TO BE FIXED TO THE RACK PERMANENTLY WITH THE TWO PANEL SCREWS.

INCORRECT USE OF THIS DEVICE, USE IN ANY OTHER ENVIRONMENT AND/OR HOUSING THAN PROVIDED BY FLEXDSL MIGHT LEAD TO HARMFUL CONDITIONS. FAILURE TO FOLLOW THESE PRECAUTIONS MAY RESULT IN DEATH, SEVERE INJURY OR PROPERTY DAMAGE.

Please read this manual carefully before operating the system.
Installation of this equipment has to be done by **qualified** personnel only.

EU DIRECTIVE 2002/96/EC AND EN50419

Our equipment is marked with the recycling symbol. It means that at the end of the life of the equipment you must dispose it separately at an appropriate collection point and not place it in the normal domestic unsorted waste stream. (European Union only)

1 PRECAUTION

The present document describes devices of the FlexDSL GigaFlex family. The document contains configuration, and operation instructions. Appendices and installation manuals containing additional information about the system are also an integral part of the present document.

WARNING
THIS EQUIPMENT IS NOT SUITABLE FOR USE IN LOCATIONS WHERE CHILDREN ARE LIKELY TO BE PRESENT.

WARNING
BEFORE STARTING OPERATING THE EQUIPMENT, READ CAREFULLY THE CURRENT MANUAL AND THE INSTALLATION MANUAL. FLEXDSL TELECOMMUNICATIONS AG REFUSES NEITHER TAKING ANY RESPONSIBILITY NOR GRANTING ANY WARRANTY TO ANY DEVICE MALFUNCTIONING OR ANY DAMAGES DUE TO FAILURE TO COMPLY WITH THE REQUIREMENTS STATED IN THE MANUALS, ESPECIALLY IN THE SECTION RELATED TO “SERVICE INSTRUCTIONS”.

WARNING
IMPROPER USE OF OUR EQUIPMENT, USE IN ANY OTHER ENVIRONMENT OR IMPROPER INSTALLATION AND MAINTENANCE MIGHT LEAD TO HARMFUL CONDITIONS. FAILURE TO FOLLOW THESE PRECAUTIONS MAY RESULT IN DEATH; SEVERE INJURY OR PROPERTY DAMAGE.
FLEXDSL TELECOMMUNICATIONS AG REFUSES NEITHER TAKING ANY RESPONSIBILITY NOR GRANTING ANY WARRANTY IN SUCH CASE.

WARNING
ELECTRONIC MODULES CAN BE DAMAGED OR DECREASED IN RELIABILITY BY STATIC ELECTRICAL DISCHARGE. BEFORE HANDLING MODULES, WEAR AN ANTISTATIC DISCHARGE WRIST STRAP TO PREVENT DAMAGE TO ELECTRONIC COMPONENTS. PLACE MODULES IN ANTISTATIC PACKING MATERIAL WHEN TRANSPORTING OR STORING. WHEN WORKING ON MODULES, ALWAYS PLACE THEM ON AN APPROVED ANTISTATIC MAT THAT IS ELECTRICALLY GROUNDED. TO PREVENT ELECTRICAL SHOCK, DO NOT INSTALL EQUIPMENT IN A WET LOCATION OR DURING A LIGHTNING STORM.

WARNING
THE PROTECTIVE GROUND CONNECTION MUST BE APPLIED TO THE UNIT. MAKE SURE THAT THE UNIT AND ALL EQUIPMENT CONNECTED TO IT USE THE SAME PROTECTIVE GROUND FOR THE PURPOSE OF REDUCING NOISE INTERFERENCE AND SAFETY HAZARDS.

2 USING THE COMMAND-LINE INTERFACE

2.1 Accessing CLI

The Command Line Interface (CLI) can be locally accessed over USB Type mini B female connector or over the first RS-232 interface, if present. Default LCT settings are:

- Rate: 9600 bps
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: Off

Remote access to the CLI can be done either through Telnet or over SSH protocols. Default IP Address is 192.168.0.235/24.

Default username is admin, default password is admin.

2.2 CLI Conventions

The syntax of CLI commands is given in `Courier New Font`.

Elements in `(< >)` indicate the field required as input along with a CLI command, for example, `<integer (100-1000)>`.

Elements in square brackets `([])` indicate optional fields for a command.

Text in `{}` refers to a group of tokens separated by a `|` symbol. One of these tokens must be mandatory selected

The `no` form of the command resets a configuration to its default value or revokes the setting. This is explicitly explained in the description of the commands for which it is applicable.

The CLI uses the following Keyboard Shortcuts:

- Up Arrow / Down Arrow: Displays the previously executed command.
- Backspace / Ctrl + H: Removes a single character.
- TAB: completes a command without typing the full word. The autocompletion works if a typed sequence can be uniquely recognized.
- Left Arrow / Right Arrow: Traverses the current line.
- ?: list available commands or options
- q: stops multi-page command output if `--More--` is shown.

2.3 Getting Help

The CLI offers context sensitive help. The user can type a question mark `(?)` anytime during a session to get help.

The user can follow by the question mark any command:

```
# con?
configure
```

or the user enters a keyword at the command prompt and enters a question mark after hitting a space:

```
(configure)# service ?
dhcp                  DHCP related configuration
dhcp-relay            DHCP relay related configuration
dhcp-server           DHCP server related configuration
```

2.4 Command Line Modes

The Figure 2-1 represents possible CLI command modes:

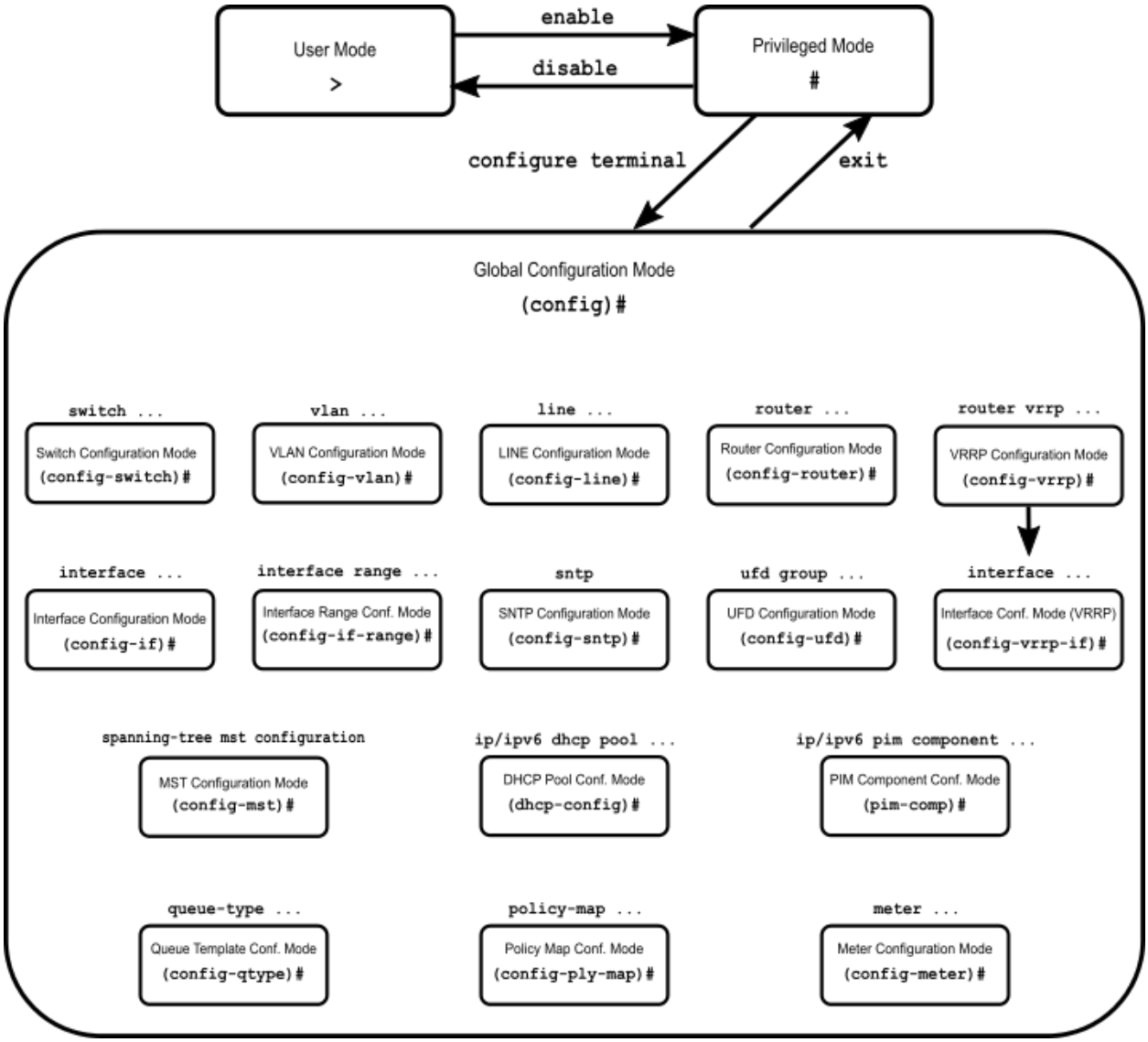


Figure 2-1. Command Line Modes.

Commands `enable` and `disable` allows change between User and Privileged Mode. Command `configure terminal` enters Global Configuration Mode. Command `exit` returns the CLI to the previous level. Commands written above blocks inside the Global Configuration Mode change CLI to the specified mode.

Command `end` returns the CLI to the Privileged Mode from any Mode directly.

3 USING WEB-GUI

3.1 Accessing Build-in WEB Server

The build-in WEB Server can be accessed by entering a unit IP address in the address line of a WEB-browser. The IP address of the unit can be found with `show ip interface` command from Privileged Mode. Default IP Address is 192.168.0.235/24.

Default user name is admin, default password is admin.

The HTTP server can be enabled or disabled with the following command available in Global Configuration Mode:

```
set ip http {enable | disable}
```

The server status and port can be shown with the following command in the Privileged or un User Mode:

```
show http server status
```

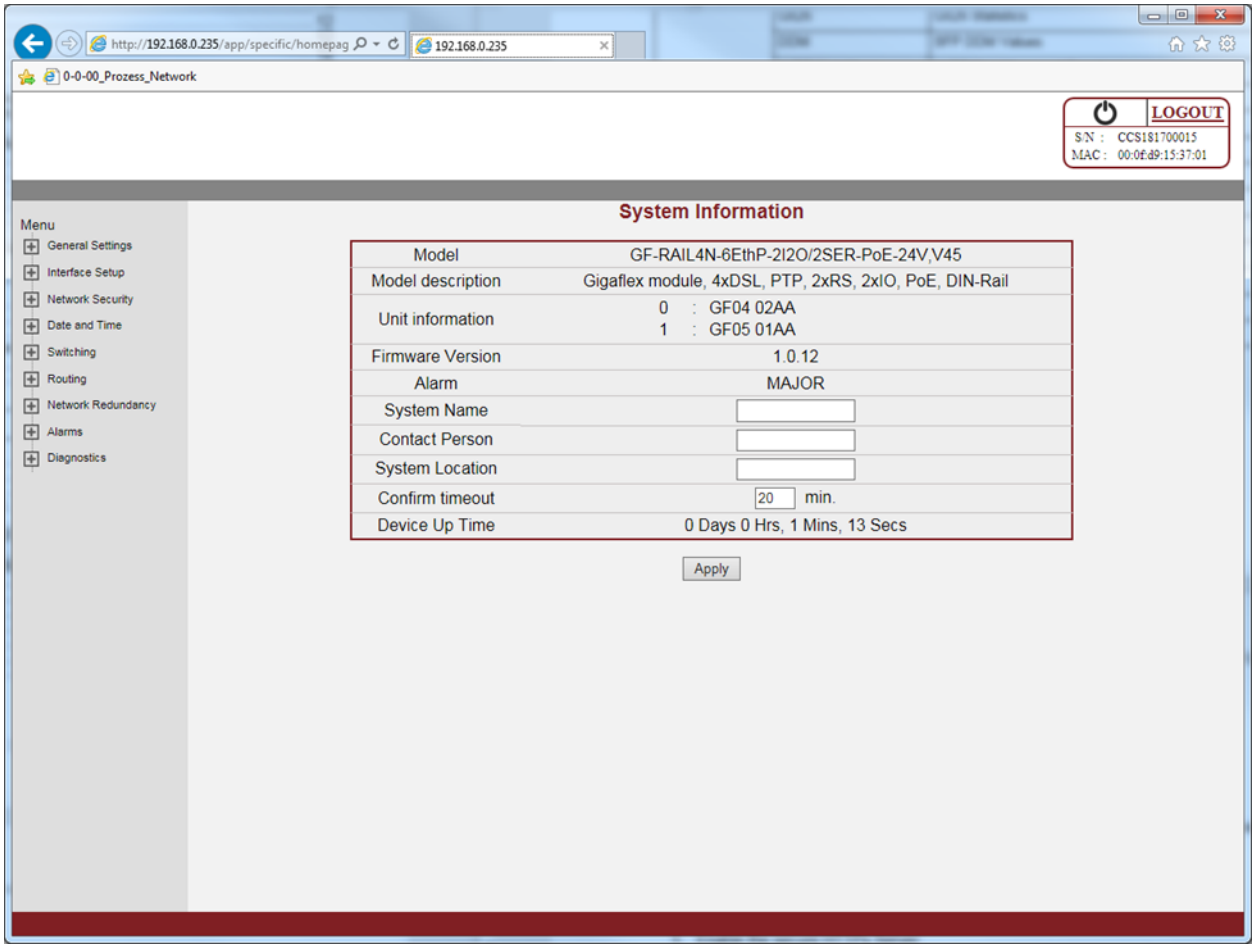
3.2 WEB Interface Structure

The build-in WEB interface has the following structure:

Menu	Sub-Menu	Description
General Settings	System	System Information
	Network IPv4	IPv4 Configuration
	Network IPv6	IPv6 Configuration
	Entity MIB	Entity MIB
	Network Discovery	LLDP Configuration
	Services	HTTPs, SSH and SNMP settings
	Software, Config Tools	Software Upgrade, Save, Restore and Erase Configuration
	Licenses	Adding or Removing Software Licenses
Înterface Setup	Ethernet Settings	Port Basic Settings, Speed, Duplex and FlowControl setup
	DSL	DSL Configuration
	IO	Digital Input and Output Configuration
	RS-232(485)	Serial Interface Configuration
	Power over Ethernet	Power over Ethernet Configuration
Network Security	802.1x	802.1x Settings
	VPN	VPN Setup
	IPSec	IP Security Setup
	ACL	MAC or IP Access List Configuration
Date and Time	SNTP	System Date and Time and SNTP settings
Switching	VLAN	VLAN and GVRP configuration
	Multicast	IGMP Configuration

Menu	Sub-Menu	Description
	QoS Ingress	QoS Ingress Configuration
	QoS Egress	QoS Egress Configuration
	IGMP Snooping	IGMP Snooping Configuration
Routing	Static Routes	Static Routes Configuration, IPv4 and IPv6
	RIP	RIP Configuration, IPv4
	OSPF	OSPF parameters Configuration, IPv4 and IPv6
	NAT	Network Address Translation Configuration
	RRD	Route Redistribution Configuration
	Multicast	PIM Configuration
Network Redundancy	Spanning Tree	Spanning Tree Configuration
	Link Aggregation	Link Aggregation Configuration
Alarms	Common	Alarm Trap, Interface Alarm Status and Configuration
	DSL	DSL Alarm Status and Configuration
	IO	Input and Output Status and Configuration
	RS-232(485)	Serial Interface Status and Alarm Configuration
Diagnostics	Network	TCP, UDP Counters, ARP Cache
	Ethernet	Ethernet Counters
	G826	G826 Statistics
	DDM	SFP DDM Values
	LLDP Neighbors	LLDP Neighbors and Counters
	802.1x	802.1x Session and Supplicant Statistics
	VPN	VPN Statistics
	VLAN	VLAN Counters
	MRP	MRP Statistics
	QoS	QoS Counters
	RIP	RIP Interface Statistics
	OSPF	OSPF Route Information and Counters
	Spanning Tree	Spanning Tree Statistics and Counters
	Link Aggregation	Link Aggregation Statistics and Counters
	Multicast	Various Multicast Statistics

3.3 WEB Interface Overview



3.4 Secure Access to the WEB Server

The build-in WEB Server support secure connection over HTTPs protocol. Network administrator should follow these steps for enabling the HTTPs on the device:

1. Generate SSL Private Key
2. Generate Certificate Request
3. Sign the Certificate Request
4. Enter the resulting Certificate into the device.
5. Enable the secure HTTPs Server.

The following commands activate HTTPs.

The `ip http secure` command enables SSL server on the device and configures cipher suites and crypto keys.

The no form of the command disables SSL server on the device and disables cipher suites and crypto key configuration.

```
ip http secure { server |  ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-
sha]  [rsa-3des-sha] [dh-rsa-des-sha ][dh-rsa-3des-sha][rsa-exp1024-des-sha]  [r
sa-with-aes-128-cbc-sha] [rsa-with-aes-256-cbc-sha]  [dhe-rsa-with-aes-128-cbc-s
ha] [dhe-rsa-with-aes-256-cbc-sha]|  crypto key rsa [usage-keys (512|1024|2048)] }
```

Parameter	Description
server	Configures the server status to be enabled. When the server status is enabled it establishes the secure layer in the network.

ciphersuite	Configures the ciphersuite for providing the input. When an SSL connection is established, the client and server exchange information about which cipher suites they have in common. Default cipfersuite is rsa-des-sha:rsa-3des-sha:rsa-exp1024-des-sha.
crypto key rsa	Configures the usage key (512, 1024 or 2048). After execution of this command the private key will be generated.

This command must be executed in the Global Configuration Mode.

The `ssl gen cert-req` command generates the Certificate Request for the defined Subject Name

```
ssl gen cert-req algo rsa sn <SubjectName>
```

Parameter	Description
SubjectName	Is an IP Address or Domain Name of the unit you want to create a certificate for.

This command must be executed in the Privileged Mode.

The `ssl server-cert` command allows signed Certificate entry into the device.

This command must be executed in the Privileged Mode.

The `set ip http` command allows activation or deactivation of the unsecured HTTP server. Usage:

```
set ip http {enable | disable}
```

Parameter	Description
enable	HTTP Server is working.
disable	HTTP Server is disabled.

This command must be executed in the Global Configuration Mode.

The `ip http port` command sets the HTTP port. The no form of the command resets the HTTP port to its default value. Usage:

```
ip http port <port(1-65535)>
```

Parameter	Description
port (1-65535)	HTTP Server working Port. Defaultvalue is 80.

This command must be executed in the Global Configuration Mode.

The following commands allow the Network Administrator to check the status of HTTP or HTTPs servers:

```
show http server status
show ip http secure server status
```

Both commands can be executed in the User or in Privileged Mode.

HTTPs can be activated through WEB interface. The corresponding dialogs are located on the General Settings → Services Page.

4 ADMINISTERING THE UNIT

4.1 Configuring LCT Console Access

Local craft Terminal (LCT) configuration options become available after typing `line console` command in Global Configuration Mode. These commands are listed below:

```
baudrate                        set baudrate
mirror rs                       console mirror mode
exec-timeout                    Configures EXEC timeout (in seconds) for
                                line disconnection
```

The `baudrate` command sets baud rate for LCT. It has the following syntax:

```
baudrate (150|300|600|1200|2400|4800|9600|14400|19200|28800|38400|56000|57600|
115200|230400)
```

Parameter	Description
Rate	Console rate in bps. Default speed is 9600 bps

The `mirror rs` command allows to mirror input and output between USB and RS-232 interfaces. It has the following syntax:

```
mirror rs [{ 1 | 2 }]
```

Parameter	Description
1 | 2	Indicates RS-232 Interface number. Default settings is RS-232 #1 is mirrored with USB. Note that the RS-232 interface must be in shutdown state before applying mirroring.

The `no mirror rs` command removes mirroring feature.

The exec-timeout command defines period of inactivity for console to be closed. It has the following syntax:

```
exec-timeout <integer (1-18000)>
```

Parameter	Description
1-18000	Defines period of inactivity in seconds. Default value is 1800.

The `no exec-timeout` command restores default value for this parameter.

These commands can be executed in Line Configuration Mode.

The `show line console` command displays the actual line console configuration. It is available either in User or in Privileged Mode.

4.2 Assigning IP Address

The IPv4 or IPv6 Address may be assigned on the interface or on the VLAN. If an IP address should be assigned on the interface, this interface must be configured as Router Port with `no switchport` command.

The GigaFlex software supports multiple IP Addresses, any of them can be used for remote inbound management of the device.

NOTE: Default IP Address of the unit is 192.168.0.235/24; it's manually assigned on the VLAN1, enabled on all ports.

4.2.1 Manual Configuration

IPv4 Address can be manually assigned on the interface or on the VLAN with the help of the following command:

```
ip address <ip-address> <subnet-mask> [secondary]
```

Parameter	Description
ip-address	IP Address in Dot-decimal notation
subnet-mask	Subnet Mask in Dot-decimal notation
secondary	Optional field allowing to set secondary IP address on an interface.

IPv6 Address can be manually assigned on the interface or on the VLAN with the help of the following commands:

```
ipv6 address <prefix> <prefix Len> [{unicast | anycast | eui64}] [cga]
ipv6 address <prefix> link-local [cga]
```

Parameter	Description
prefix	Configures IPv6 prefix for an interface.
prefix Len	Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges from 0 to 128.
unicast	Configures the address type of the prefix as Unicast.
anycast	Configures the address type of the prefix as Anycast.
eui64	Configures the type of Prefix where the latter 64 bits are formed from the link layer address.
cga	Option tells the system to assign Cryptographically Generated Address. Note: RSA key should be generated before assigning a CGA address. Secure Network Discovery should be enable in either secured or mixed mode before making the address type as CGA.
link-local	This command configures the IPv6 link-local address on the interface. The link-local address is an IP address that is intended only for communications within the segment of a local network or a point-to-point connection.

The “no” version of these commands removes IP Address entry from an interface.

These commands can be executed in the Interface Configuration Mode or in the Interface VLAN Configuration Mode.

4.2.2 DHCP Client

An IPv4 or IPv6 Address of an interface or of an VLAN can be automatically assigned from DHCP Server. The following commands can be used for this purpose:

```
ip address dhcp
ipv6 address dhcp
```

Parameter	Description
ip address dhcp	Tells the system to obtain the IPv4 Address from an DHCP Server for an interface.
ipv6 address dhcp	Tells the system to obtain the IPv6 Address from an DHCP Server for an interface.

The “no” version of this command removes IP Address allocation from an interface or VLAN.

These commands can be executed in the Interface Configuration Mode or in the Interface VLAN Configuration Mode.

4.3 System Date and Time

4.3.1 Manual Configuration

The System Clock can be manually configured with `clock set` command in Privileged Mode:

```
clock set hh:mm:ss <day (1-31)> {<month (01-12)> | january | february | march
| april | may | june | july | august | september | october | november | december
} <year (2000 - 2037)>
```

Parameter	Description
hh:mm:ss	Hours, minutes and seconds.
Month	Month’s sequence number or name of the month.
Year	Year in range from 2000 to 2037

System Clock can be shown with `show clock` command in User or Privileged Mode.

System Clock can be configured in WEB on Date and Time page.

4.3.2 SNTP

System Clock can be automatically configured from SNTP Server. The configuration can be done in SNTP Configuration Mode by entering command `sntp` in Global Configuration Mode:

```
(config)# sntp
(config-sntp)#
```

SNTP parameters can be configured in WEB on Date and Time → SNTP page.

4.3.2.1 Set SNTP Client

This command enables or disables SNTP Client on the device and configures various client parameters:

```
set sntp client {enabled | disabled}
set sntp client clock-format {ampm | hours}
set sntp client time-zone <UTC-offset value as (+HH:MM /-HH:MM)(+00:00 to +14:00)/ (-00:00 to -
12:00)>
no sntp client time-zone
set sntp client clock-summer-time <week-day-month,hh:mm> <week-day-month,hh:mm>
no sntp client clock summer-time
set sntp client authentication-key <key-id> md5 <key>
no sntp client authentication
set sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <dns_host_name>}
[{primary | secondary}]
no sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <dns_host_name>}
```

Parameter	Description
enabled	Enables SNTP Client
disabled	Stops SNTP client
clock-format	Changes Clock format between AM/PM and Hours
time-zone	Set UTC clock offset. The no version of this command removes configuration entry.

clock-summer-time	Set Daylight Saving Time parameters. The no version of this command removes configuration entry.
authentication key	Set MD5 authentication key with key-id from 1 to 65535. The no version of this command removes configuration entry.
unicast-server	Sets the IPv4 or IPv6 SNTP Server. The no version of this command removes configuration entry.

These commands are available in SNTP Configuration Mode.

4.3.2.2 Show SNTP

This command displays SNTP parameters and shows system clock:

```
show sntp clock
show sntp status
show sntp unicast-mode status
```

Parameter	Description
clock	Shows SNTP Clock. This command is equil to show clock command.
status	This command displays SNTP status.
unicast-mode status	This command displays the status of SNTP in unicast mode

These commands can be executed in User / Privileged Mode

4.4 System Name, Location and Contact

System name, location or contact can be configured either in CLI or in WEB on General Settings → System page.

4.4.1 Hostname

This command allows System Name allocation:

```
hostname <switchname>
```

Parameter	Description
<switchname>	Configures System Name. Type “” to erase it.

This command can be executed in the Global Configuration Mode.

4.4.2 System Contact | Location

This command configures system contact and system location:

```
system contact <contact info>
system location <location name>
```

Parameter	Description
contact	Configures system contact as it’s written in <contact info>. Type “” to erase it.
location	Configures system location as it’s written in <location name>. type “” to erayse it.

This command can be executed in the Global Configuration Mode.

NOTE:	Hostname, location and contact allows spaces. Use quotes “ ” for that purpose.

4.5 Alarm Configuration

The following commands define Alarm severity for various system features and components:

4.5.1 Alarm DSL

This command configures alarm severity for DSL Group and has the following syntax:

```
alarm dsl {trn | los | losw | ber-h | nm | la | rlos | rlosw | rber-h | rnm | rla} [port
<integer(1-4)>] {major | minor}
```

Parameter	Description
trn	Set the severity level for the event “Training”. Default: Major.
los	Set the severity level for the event “Loss of Signal”. Default: Major.
losw	Set the severity level for the event “Loss of Word”. Default: Major.
ber-h	Set the severity level for the event “Bit Error Rate – High”. Default: Major.
nm	Set the severity level for the event “Noise Margin Threshold reached”. Default: Minor.
la	Set the severity level for the event “Link Attenuation Threshold reached”. Default: Minor.
rlos	Set the severity level for the event “Loss of Signal on Remote End”. Default: Major.
rlosw	Set the severity level for the event “Loss of Word on Remote End”. Default: Major.
rber-h	Set the severity level for the event “Remote Bit Error Rate – High”. Default: Major.
rnm	Set the severity level for the event “Remote Noise Margin Threshold reached”. Default: Minor.
rla	Set the severity level for the event “Remote Link Attenuation Threshold reached”. Default: Minor.
port	DSL Interface number.
major | minor	Set Major or Minor severity level for the defined event.

This command can be executed in the Global Configuration Mode.

4.5.2 Alarm Ethernet Ifdown

This command configures the alarm severity for an Ethernet Interface Link Up / Link Down event. It has the following syntax:

```
alarm ioip {in-down | in-active | out-down | out-active} [port <integer(1-2)>] {major |
minor}
```

Parameter	Description
port	Ethernet Port Number.
major | minor	Set Major or Minor severity level for the defined event. Default settings are: Gi 0/1-2 (SFP) – Major; Gi 0/3-6 (GE) – Minor.

This command can be executed in the Global Configuration Mode.

4.5.3 Alarm IOIP

This command configures the alarm severity for Input and Output activity events. It has the following syntax:

```
alarm ioip {in-down | in-active | out-down | out-active} [port <integer(1-2)>] {major |
minor}
```

Parameter	Description
in-down	Input Interface configured, but the TCP connection is down. Default: Minor.
in-active	Current detected for an Input. Default: Minor.
out-down	Output Interface configured, but the TCP connection is down. Default: Minor.
out-active	Output Relay is in active state. Default: Minor.
port	Input or Output interface number. Default: Minor.
major | minor	Set Major or Minor severity level for the defined event.

This command can be executed in the Global Configuration Mode.

4.5.4 Alarm Power

This command configures the alarm severity for an event, caused by a power failure. It has the following syntax:

```
alarm power {v-in | rpf | rleak} [port <integer(1-2)>] {major | minor}
```

Parameter	Description
v-in	Input Voltage failure severity. Default: Minor.
rpf	Remote Power Failure severity (this feature is currently not supported). Default: Major.
rleak	Remote Power Current Leak Failure severity (this feature is currently not supported). Default: Minor.
port	Power Input number.
major | minor	Set Major or Minor severity level for the defined event.

This command can be executed in the Global Configuration Mode.

4.5.5 Alarm RSIP

This command configures the alarm severity for an event, caused by an RSoIP failure. It has the following syntax:

```
alarm rsip {down | cable} [port <integer(1-2)>] {major | minor}
```

Parameter	Description
down	The interface is configured, but the TCP connection is down. Default: Minor.
cable	The cable is not connected (this feature is currently not supported). Default: Minor.
port	Serial Interface number.
major | minor	Set Major or Minor severity level for the defined event.

This command can be executed in the Global Configuration Mode.

4.5.6 Alarm Software

This command configures the alarm severity for an event, caused by the software or configuration issues. It has the following syntax:

```
alarm software {sw-nconf | nconf | sd-snapshot} {major | minor}
```

Parameter	Description
sw-nconf	Software loaded, but not confirmed. Default: Minor.
nconf	Configuration has changed, but not confirmed. Default: Minor.
sd-snapshot	The SD-Card content don't match the device configuration and (or) firmware version. Default: Minor.
major | minor	Set Major or Minor severity level for the defined event.

This command can be executed in the Global Configuration Mode.

4.5.7 Alarm Cut-Off

This command disables alarm indication for an event. The no version of this command enables the alarm indication back. This command has the following syntax:

```
alarm cut-off software
alarm cut-off {ethernet | dsl | rsip | ioip | power} [port <integer(1-6)>]
no alarm cut-off software
no alarm cut-off {ethernet | dsl | rsip | ioip | power} [port <integer(1-6)>]
```

Parameter	Description
software	Masks the software- and configuration-related alarm events.
ethernet	Masks the Ethernet-related alarm events.
dsl	Masks the DSL-related alarm events.
rsip	Masks the RSoIP-related alarm events.
ioip	Masks the IOoIP-related alerm events.
power	Masks the Power-related alarm events.
port	Interface number.

This command can be executed in the Global Configuration Mode.

5 SOFTWARE LICENSE MODEL

The GigaFlex software structure supports additional features, protected by the license keys. The license keys are unique and can't be transferred from one device to another. The following features can be opened with license keys:

Feature Name	Description
Extended Rates	Opens TC-PAM 4/8/64/128 modulation.
IPSec	Opens IPSec and VPN.

Licenses can be managed either in CLI or in WEB on General Settings → Licenses page.

5.1 Show License

This command displays the information about activated licenses and device uuid:

```
show license { uuid | all }
```

Parameter	Description
uuid	Shows the Universal Unique Identifier of the device. This code should be sent to the manufacturer for obtaining the license key.
all	Shows information about available and active licenses.

This command can be executed in User or in Privileged Mode.

5.2 License

This command adds or removes license from the device.

```
license { add <key> | delete <option_name> }
```

Parameter	Description
add	Add the license key into the system.
delete <option_name>	Removes license with defined Option Name from the system.

This command can be executed in Global Configuration Mode.

The unit must be restarted for the license to apply.

6 FIRMWARE AND APPLICATION STORAGE

6.1 Main and Backup Firmware

The GigaFlex software support two firmware images: main and backup. If, due to any reason, the system can't boot from the main firmware image, the backup image will be used for boot process.

6.1.1 Firmware Upgrade

The `firmware upgrade` command upgrades main or backup firmware image from various sources. The command has the following syntax:

```
firmware upgrade [ md5 <string(32)> ] [ reload ] { tftp://server/filename | sftp://<user-
name>:<pass-word>@server/filename | sdcard: [filename] | usbstick: [filename] }
```

Parameter	Description
md5	MD5 sum; an error will be shown if entered value don't match with calculated value of the downloaded image.
reload	Tells system to reboot automatically after firmware download
tftp:// sftp://	Indicates TFTP or SFTP server address, credentials and file name to download.
sdcard: usbstick:	Tells system to download firmware image from SD card or USB stick.

This command can be executed in Privileged Mode.

The `firmware upgrade` command always upgrades backup image and set "boot" flag on it. The just-downloaded image will be used during next boot. The `show system information` command displays running and backup images as well as boot flag:

Initial configuration:

```
Firmware 1 version (running)   (boot)  : 1.0.0
Firmware 2 version (backup)            : 1.0.0
```

New firmware downloaded:

```
Firmware 1 version (running)           : 1.0.0
Firmware 2 version (backup)    (boot)  : 1.1.0
```

The unit was restarted:

```
Firmware 1 version (backup)            : 1.0.0
Firmware 2 version (running)   (boot)  : 1.1.0
```

Now the user can upgrade the first firmware image:

```
Firmware 1 version (backup)    (boot)  : 1.1.0
Firmware 2 version (running)           : 1.1.0
```

… and restart the unit again:

```
Firmware 1 version (running)   (boot)  : 1.1.0
Firmware 2 version (backup)            : 1.1.0
```

6.1.2 Switching Between Firmware Images

It's possible to switch working image manually. The `firmware switch image` command is used for this purpose. It has the following syntax:

```
firmware switch image [{ 1 | 2 }]
```

Parameter	Description
1 | 2	Tells system what image must be used during next boot.

This command can be executed in Privileged Mode.

6.2 Running, Backup and Startup Configuration

The GigaFlex software support three configuration storages: running, backup and startup.

- running configuration is executed now;
- backup configuration is reserved;
- startup configuration will be executed during next boot.

The two commands: `copy` and `write running-config` can be used for configuration storage management. The command `write running-config` saves running configuration to various storages; the command copy copies configuration from various storages into startup configuration. These commands have the following syntax:

```
write running-config { startup-config | backup-config | tftp://server/filename | sftp://<user-
name>:<pass-word>@server/filename | sdcard: [<filename>] | usbstick: [<filename>] }

copy { backup-config | tftp://server/filename | sftp://<user-name>:<pass-word>@server/filename
| sdcard: <filename> | usbstick: <filename> } startup-config
```

Parameter	Description
running-config	Actual configuration
backup-config	Reserved configuration
startup-config	The configuration to be used during next boot
tftp:// sftp://	Indicates TFTP or SFTP server address, credentials and file name to download or upload.
sdcard: usbstick:	Indicates SD card or USB stick to be used for upload or download configuration.

The three commands: `show running-config`, `show backup-config` and `show startup-config` can be used to display respectively: actual, reserved and startup configuration.

The startup or backup configuration can be removed with `erase` command that has the following syntax:

```
erase { startup-config | backup-config }
```

Parameter	Description
startup-config	Removes startup configuration. The unit will have factory-default settings after next boot.
backup-config	Removes reserve configuration from the unit.

All commands can be executed in Privileged Mode, while show commands can be executed either in User or in Privileged Mode.

6.3 Confirmation of Configuration Changes

The default settings of the GigaFlex software presuppose that any change to the running configuration must be confirmed, otherwise the unit will restart after predefined timeout and all not confirmed changes will be lost. This behaviour reduces influence caused by possible human mistakes, heading to the loss of remote control of the unit.

The `confirm` command writes running configuration to the startup configuration and disables reboot timer.

The `confirm timeout` command defines period in minutes after that the unit will be automatically restarted. The `no confirm timeout` command restores default period of 20 minutes. This command has the following syntax:

```
confirm timeout <integer(0-60)>
```

Parameter	Description
integer (0-60)	Sets timeout in minutes before system reboot. 0 – disables reboot timer, so no confirmation is needed. Default value is 20 minutes.

These commands can be executed in Global Configuration Mode.

User can display confirm timeout settings with `show running-config confirm` command. It's available either in User or in Privileged Mode.

6.4 Saving and Restoring System Snapshot on SD Card

The GigaFlex software can save and restore snapshot image on the SD Card. This SD Card can be used for system recovery. For example, if been inserted into new, non-programmed unit, the unit will download firmware and configuration from SD Card without any operator's actions. The following two commands operates with SD Card snapshots:

The `sdcard snapshot autorestore` command and `sdcard` snapshot. They have the following syntax:

```
sdcard snapshot autorestore { enable | disable }
sdcard snapshot { create | erase }
```

Parameter	Description
enable | disable	Enables or disables the complete system restore from SD Card during next boot.
create	Creates complete system snapshot containing firmware and configuration.
erase	Removes system snapshot from the SD Card.

These commands can be executed in Privileged Mode.

7 INTERFACE CONFIGURATION

7.1 Configuring Gigabit Ethernet Interfaces

Gigabit Ethernet Interfaces can be configured either through CLI or in WEB on Interface Setup → Ethernet Settings Page.

The Interface Configuration Mode for the Gigabit Ethernet can be accessed from the Global Configuration Mode by executing `interface gigabitethernet 0/x` command or `interface range 0/x-y` command.

The following commands can be executed in the Interface Configuration Mode:

7.1.1 Alias

This command assigns an Alias for an interface:

```
alias <string(63)>
```

Parameter	Description
<string (63)>	Interface Aliace up to 63 symbols.

7.1.2 Description

This command assigns a Description for an interface:

```
description <description of this interface>
no description
```

Parameter	Description
<description>	Interface Description. The no version of this command removes interface description.

7.1.3 Downstream Arp-Bcast

This command allows or denies the ARP Broadcast distribution in egress direction on this interface:

```
downstream arp-bcast {allow | drop}
```

Parameter	Description
allow	Allows the downstream arp bcast packet incoming on this port.
drop	Drops the downstream arp bcast packet incoming on this port.

The ARP broadcast forwarding rule can be shown with `show arp spoofing` command in User/privileged Mode.

7.1.4 Duplex

This command configures Duplex parameters of an interface:

```
duplex { full | half }
no duplex
```

Parameter	Description
full	Port is in full-duplex mode, that is data simultaneously communicates in both directions.

half	Port is in half-duplex mode, that is data can communicate in both directions, but only in one direction at a time.

The no form of the command configures the duplex operation to the default value that is set to full.

7.1.5 Flowcontrol

This command configures flow-control feature of an interface:

```
flowcontrol { on | off }
```

Parameter	Description
on	Allows flow-control feature on the port.
off	Flow-control feature is not used.

7.1.6 Speed

This command configures speed of an interface:

```
speed {10 | 100 | 1000 | auto }
no speed
```

Parameter	Description
10 | 100 | 1000	Configures port speed 10, 100 or 1000 Mbps.
auto	Port automatically configures it's speed based on the peer switch. The switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The no parameter of the command restors default value: auto

7.1.7 Negotiation

This command turns Auto-negotiation feature on the port on and off:

```
negotiation
no negotiation
```

Parameter	Description
negotiation	Auto-negotiation is enabled. Flow-control, Duplex and Speed settings are not available in this mode.
no negotiation	Auto-negotiation is disabled.

7.1.8 MTU

This command configures MTU frame size on the interface:

```
mtu <frame-size(46-9216)>
```

Parameter	Description
frame-size	MTU size in bytes from 46 to 9216. Default value is 1536 bytes.

7.1.9 Rate-Limit Output

This command enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface.

The no form of the command disables the rate limiting and burst size rate limiting on an egress port.

```
rate-limit output [<rate-value>] [<burst-value>]
no rate-limit output [rate-limit] [burst-limit]
```

Parameter	Description
rate-value	Configures the maximum rate (in kbps) at which packets can be sent out through the interface. Default: 0
burst-value	Configures the burst size in kilobytes with which the rate is to be implemented. The value is the product of the rate and interval at which rate is to be measured. Default: 0

7.1.10 Rate-Limit Pause

This command enables the pause ingress rate limit above which PAUSE frames are transmitted on the interface.

The no form of the command disables pause ingress rate limiting on a port.

```
rate-limit pause [<high-watermark>] [<low-watermark>]
no rate-limit pause
```

Parameter	Description
high-watermark	Configures the ingress rate equal to or above which PAUSE frames are transmitted. This value ranges from 1 to 80000000 kbps. Default: 0
low-watermark	Configures the ingress rate below which transmission of PAUSE frames are stopped. This value ranges from 1 to 80000000 kbps. Default: 0

7.1.11 Shutdown

This command brings the port administrative status down and up:

```
shutdown
no shutdown
```

Parameter	Description
shutdown	The Port is administratively down (deactivated).
no shutdown	The Port is administratively up.

7.1.12 Storm-Control

This command sets the storm control rate for broadcast, multicast and DLF packets.

The no form of the command sets storm control rate for broadcast, multicast and DLF packets to the default value.

```
storm-control { broadcast | multicast | dlf } level <rate-value>
no storm-control { broadcast | multicast | dlf } level
```

Parameter	Description
level	Configures maximum rate value for broadcast, multicast and unknown unicast, or dlf (Destination Lookup Failure) traffic.

7.1.13 SFP Speed Mode

This command tells the system what kind of SFP modules are installed in the system:

```
sfp speed mode { mono | triple }
```

Parameter	Description
mono	SFP Modules are single-speed SFPs.
triple	SFP Modules are 10/100/1000 kbps SFPs.

This command can be executed in the Global Configuration Mode.

7.1.14 Network Type WAN

This command configures physical interface as a WAN interface. The no version of this command removes this feature. The WAN interface allows NAT and VPN features on the physical interface.

```
network-type wan
no network-type wan
```

This command can be executed in Physical Interface Configuration Mode (Switch or Router).

7.1.15 Show Interfaces

This command displays various parameters of all, or selected Ethernet interfaces:

```
show interfaces [<interface-type> <interface-id> ] etherchannel
show interfaces [{[<interface-type> <interface-id>] [{description | storm-control | flowcontrol
| capabilities | status | port-security-state | rate-limit}] | {vlan <vlan-id>}}]
show interfaces mtu [{Vlan <vlan-id> | port-channel <port-channel-id (1-65535)> | <interface-
type> <interface-id>}]
show interfaces statistics
show interfaces {counters | HC-counters} [{<interface-type> <interface-id> | vlan <vlan_id>| }]
```

Parameter	Description
interface-type	gigabitethernet or gi
interface-id	Slot and Port, for example 0/1
etherchannel	Show information about aggregated channels
description	Shows interface description
storm-control	Shows interface storm-control
flowcontrol	Shows interface flow-control
capabilities	Show interface capabilities: speed, duplex and flow-control
status	Show interface status
port-security-state	Show interface port-security
rate-limit	Shows interface rate-limit

vlan	Shows VLAN related information
mtu	Shows MTU value for all ar for selected interfaces or port-channels
statistics	Shows interface statistics
counters	Displays the interface statistics for all the available interfaces.
HC-counters	Displays the interface incoming and outgoing traffic statistics for the HC (High Capacity 64 bit) counters.

This command can be executed in User or in Privileged Mode.

7.2 Configuring SHDSL Interfaces

The SHDSL interfaces can be configured either through CLI or in WEB on Interface Setup → DSL page.

7.2.1 The Bonding Groups and Port Association

The GigaFlex modems support up to four DSL channels, depending on a model. Each channel has a physical connection with an internal port of the switch. The table below shows the port to DSL channel mapping for the models with four DSL channels.

Switch Port Number	DSL Channel
Gi 0/7	DSL 1
Gi 0/8	DSL 2
Gi 0/9	DSL 3
Gi 0/10	DSL 4

The table below shows the port to DSL channel mapping for the models with two DSL channels.

Switch Port Number	DSL Channel
Gi 0/7	DSL 1
Gi 0/8	DSL 2

For the star configuration over single pair per ray, every internal port must serve own DSL direction.

The point-to-point application over several pairs working in parallel is called **Bonding**. This process is controlled by the DSL chip, that distributes the data traffic between several pairs automatically. The unused internal Ethernet ports will be unused in that case.

The GigaFlex modem supports up to two bonding groups. The tables below display the Port-to-Bonding-Groups mapping and correct line protocol status of internal ports 0/7 – 0/10.

Point-to-point, four DSL channels in parallel:

Switch Port Number	Line Protocol Status	Bonding Group 1
Gi 0/7	Up	DSL 1
Gi 0/8	Down	DSL 2
Gi 0/9	Down	DSL 3

Gi 0/10	Down	DSL 4

Two Bonding Groups with two channels in each:

Switch Port Number	Line Protocol Status	Bonding Group 1	Bonding Group 2
Gi 0/7	Up	DSL 1	
Gi 0/8	Up		DSL 2
Gi 0/9	Down	DSL 3	
Gi 0/10	Down		DSL 4

Two Bonding Groups with other two channels in each:

Switch Port Number	Line Protocol Status	Bonding Group 1	Bonding Group 2
Gi 0/7	Up	DSL 1	
Gi 0/8	Down	DSL 2	
Gi 0/9	Up		DSL 3
Gi 0/10	Down		DSL 4

One Bonding Group with tree channels and one channel without Bonding:

Switch Port Number	Line Protocol Status	Bonding Group 1	Separate Channel
Gi 0/7	Up	DSL 1	
Gi 0/8	Down	DSL 2	
Gi 0/9	Down	DSL 3	
Gi 0/10	Up		DSL 4

Conclusion:

- The Bonding Group Member with the lowest DSL channel number, will have the corresponding internal Ethernet Port in line protocol status “Up”.
- The other Members of the same Bonding Groups will have their corresponding internal Ethernet Ports in line protocol status “Shutdown”.
- The independent (not bonded) DSL channels, will have their corresponding internal Ethernet Ports in line protocol status “Up”.

7.2.2 DSL-Bonding Group

This command assigns the DSL channel membership in the Bonding Group.

The no version of this command removes the DSL members from the Bonding Group.

```
dsl-bonding group <integer(1-2)> shdsl <integer(1-4)> [<integer(1-4)>] [<integer(1-4)>]
[<integer(1-4)>] [{multipair}]
no dsl-bonding group <1-2>
```

Parameter	Description
group	Selects first or second Bonding Group
shdsl	List of DSL channels separated by the space character.
multipair	Activates the multipair feature for the selected bonding group. The multipair feature disables the data transmission over all members of a bonding group if one member fails. The multipair mode is disabled by default. In this mode the fail of a member doesn't lead to the fail of the whole group that continues to forward the data traffic through the working group members.

This command can be executed in the Global Configuration Mode.

The Interface Configuration Mode for the SHDSL port can be accessed from the Global Configuration Mode by executing `interface shdsl x` command or `interface range shdsl x - y` command.

7.2.3 SHDSL-Bonding Group

This command is an alias of the `dsl-bonding group` command and has the same parameters.

7.2.4 Annex

This command configures the G.991.2 Annex A or Annex B standard for the SHDSL transmission.

```
annex { a | b | auto }
```

Parameter	Description
a	Configures G.991.2 Annex A
b	Configures G.991.2 Annex B
auto	Configures G.991.2 Annex automatically

7.2.5 Baserate

This command defines the rate of a SHDSL channel

```
baserate {<3-238> | auto }
```

Modulation	Allowed Rates
PAM 4 (Extended)	3 … 39
PAM 8 (Extended)	3 … 79
PAM 16	3 … 60
PAM 16 (Extended)	3 … 119
PAM 32	12 … 89
PAM32 (Extended)	3 … 159
PAM 64 (Extended)	3 … 199
PAM 128 (Extended)	4 … 238

auto	Automatic rate adaptation (not for Extended modes)

7.2.6 Extended

This command activates Extended Modulations and require License Key

```
extended { disable | enable }
```

Parameter	Description
disable	Extended Mode is disabled
enable	Extended Mode is enabled

7.2.7 Master

This command switches SHDSL operation Mode between Master and Slave

```
master { on | off | auto}
```

Parameter	Description
on	SHDSL is in Master Mode
off	SHDSL is in Slave Mode
auto	automatically select Master or Slave mode for an SHDSL

7.2.8 PAM

This command defines SHDSL Modulation

```
pam { 4 | 8 | 16 | 32 | 64 | 128 | auto }
```

Parameter	Description
value	Set PAM Modulation according to defined value
auto	Set PAM Modulation Automatically (only if Extended Mode is disabled)

7.2.9 Threshold

This command sets the threshold for Noise Margin or Link Attenuation when the SNMP Trap should be generated.

```
threshold {noise-margin | link-attenuation} {<0-25> | disabled}
```

Parameter	Description
noise-margin	Set Noise Margin Threshold
link-attenuation	Set Link Attenuation Threshold
value	Set threshold Value for an Alarm and SNMP Trap
disabled	Deactivates the Threshold

7.2.10 Shutdown

This command brings SHDSL Interface administratively down and up. All SHDSL-related parameters, except command `set`, can be changed for an interface in shutdown state and will be applied as soon as the interface will become administratively up.

```
shutdown
no shutdown
```

Parameter	Description
shutdown	Set SHDSL Interface administratively down. All parameters can be changed in this mode.
no shutdown	Set SHDSL Interface administratively up. All parameters will be applied in this mode.

7.2.11 Set Baserate PAM Extended

This command allows parameters application to the interface without bringing it to the Shutdown state first.

```
set [baserate {<integer(3-238)> | auto}] [pam {"4" | "8" | "16" | "32" | "64" | "128" | auto}]
[extended {disable | enable}]
```

Parameter	Description
baserate	Set line rate for an interface or interfaces. Refer to the rules described in the Chapter 7.2.5 Baserate for correct settings.
pam	Set modulation as PAM4 … PAM128 or auto
extended	Enables or disables the Extended Rates.

7.2.12 Show SHDSL

This command displays SHDSL configuration and status.

```
show shdsl
show shdsl g826 [{ local | remote }]
show shdsl status
```

Parameter	Description
shdsl	Displays SHDSL configuration
g826	Show G.826 Statistics for the local or for the remote unit
status	Display SHDSL Status

This command can be executed in User or in Privileged Mode.

7.3 Configuring Serial Interfaces

The Serial Interface configuration can be done either through CLI or in WEB on Interface Setup → RS-232(485) page.

The Interface Configuration Mode for the Serial port can be accessed from the Global Configuration Mode by executing `interface rs x` command.

7.3.1 Baudrate

This command configures rate of the Serial interface

```
baudrate (150|300|600|1200|2400|4800|9600|14400|19200|28800|38400|56000|57600|115200|230400)
```

Parameter	Description
value	Set Serial Interface working rate

7.3.2 Filter

This command enables the security filter for the incoming packets.

```
filter { on | off }
```

Parameter	Description
on	Receiver will check if the incoming packet came from known source, configured in remote IP table. If a source is known, the packet will be forwarded to the serial interface, otherwise a packet will be dropped.
off	Incoming filtering is disabled. Any incoming packet will be forwarded to the serial interface. This is the default value.

7.3.3 Format

This command configures Format of the Serial interface.

```
format [bits (7-8)] [parity {none|odd|even}] [stopbits {1|1.5|2}]
```

Parameter	Description
bits	Number of Data bits: 7 or 8
parity	Parity: None, Odd or Even
stopbits	Number of Stop bits: 1, 1.5 or 2

7.3.4 Local Port

This command configures the listening port for incoming IP packets.

```
local port <1-65535>
```

Parameter	Description
value	IP Port the Server listens on.

7.3.5 Loop

This command configures local or remote loopback on the serial interface.

The no version of this command removes local or remote loopback from an interface.

```
loop {1 | 2}
no loop {1 | 2}
```

Parameter	Description
1	Enables local loopback heading to the terminal equipment.
2	Enables remote loopback heading to the packet network.

7.3.6 Protocol

This command configures RS over IP transport: UDP or TCP. For TCP transport this command configures server or client role.

```
protocol { tcp {client | server} | udp }
```

Parameter	Description
tcp client	Configures TCP transport und client role

tcp server	Configures TCP transport und server role
udp	Configures UDP transport

7.3.7 Remote IP

This command configures IPv4 address and port of a peer.

The no version of this command removes remote IP address from a table of peers

```
remote ip <ip address> port <1-65535>
no remote ip <ip_addr> port <1-65535>
```

Parameter	Description
ip address	IPv4 Address in DDN format
port	Port a peer listens on

7.3.8 Signaling

This command configures CTS/RTS signalling behaviour.

```
signaling { off | local | remote }
```

Parameter	Description
off	CTS/RTS signals are ignored.
local	Local CTS follows local RTS
remote	Local CTS follows remote RTS

7.3.9 Type

This command configures the Type of the Serial Interface.

```
type {232 | {{ 422 | 485 [mode {half | full}] } [term {off | on}]}}
```

Parameter	Description
232	Serial interface type is RS-232
422	Serial interface type is RS-422
485	Serial interface type is RS-485
mode	Sets half or full duplex mode for RS-422/485 interface
term	Sets interface termination for RS-422/485 interface

7.3.10 Shutdown

This command brings Serial Interface administratively down and up. All Serial-related parameters can be changed for an interface in shutdown state and will be applied as soon as the interface will become administratively up.

```
shutdown
no shutdown
```

Parameter	Description
shutdown	Set Serial Interface administratively down. All parameters can be changed in this mode.

no shutdown	Set Serial Interface administratively up. All parameters will be applied in this mode.

7.3.11 Show RS

This command shows information and status of Serial interface.

```
show rs
show rs signaling [<1-2>]
show rs statistics [<1-2>]
```

Parameter	Description
rs	Shows Serial interface configuration.
signaling	Shows RTS and CTS statuses
statistics	Shows Serial interface statistics

This command can be executed in User or in Privileged Mode.

7.4 Configuring IO Lines

The digital Input or Output lines can be configured either through CLI or in WEB on Interface Setup → IP page.

The Interface Configuration Mode for the IO lines can be accessed from the Global Configuration Mode by executing `interface io {in | out} <1-2>` command.

7.4.1 Alarm Trigger

This command configures Alarm severity that triggers the Output interface.

```
alarm trigger { nonurgent | urgent } normalstate { open | close }
```

Parameter	Description
trigger	Tells the system what alarm should change the Output state: Urgent or Nonurgent.
normalstate	Configures if the Output should be open or closed without alarm

7.4.2 Force

This command forces Input and Output state.

The no version of this command removes forced state.

```
force { open | close }
force { open | close | alarm }
no force
```

Parameter	Description
Open	Configures Input or Output state as Open.
Close	Configures Input or Output state as Close.
alarm	Configures Output state as Alarm present.

7.4.3 Insensitivity

This command adds insensitivity interval for an Input.

The no version of this command removes the insensitivity delay.

```
insensitivity time <100-10000>
no insensitivity
```

Parameter	Description
time	Adds the insensitivity delay in miliseconds.

7.4.4 Local Port

This command configures the listening port for incoming IP packets.

```
local port <1-65535>
```

Parameter	Description
port	IP Port the Server listens on.

7.4.5 Remote IP

This command configures IPv4 address and port of a peer. This command is available only for Input.

The no version of this command removes remote IP address from a table of peers

```
remote ip <ip address> port <1-65535>
no remote ip <ip_addr> port <1-65535>
```

Parameter	Description
ip address	IPv4 Address in DDN format
port	Port a peer listens on

7.4.6 Protocol

This command configures IO over IP transport: UDP or TCP.

```
protocol { tcp | udp }
```

Parameter	Description
tcp	Configures TCP transport.
udp	Configures UDP transport

7.4.7 Type

This command configures the Normally-Open or Normally-Closed Type of the Input.

```
type {no | nc}
```

Parameter	Description
no	Tells the system that this Input is normally opened
nc	Tells the system that this Input is normally closed

7.4.8 Show IO

This command displays the IO configuration and statistics.

```
show io
```

```
show io statistics [<1-4>]
```

Parameter	Description
io	Shows IO configuration
statistics	Shows IO statistics

This command can be executed in User or in Privileged Mode.

7.5 Configuring PoE

Power over Ethernet technology transmits electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. The advantage of this technology is that the installers need to run only a single Ethernet cable that carries both power and data to each device. IP telephones, wireless LAN access points, webcams, Ethernet hubs, computers, and other appliances use this technology. Access Points and network devices can be easily located, decreasing installation costs in many cases.

Power over Ethernet can be configured trough CLI or in WEB on Interface Setup → Power over Ethernet page.

7.5.1 Set PoE

This command enables/disables Power Over Ethernet module in the unit.

```
set poe {enable | disable}
```

Parameter	Description
enable	Enables the Power Over Ethernet module in the unit.
disable	Disables the Power Over Ethernet module and releases all the resources allocated to the POE module to the system and the power is shut off on all POE enabled ports.

This command can be executed in in Global Configuration Mode.

7.5.2 Power Inline

This command enables/disables Power Over Ethernet on the specified port to provide power over a copper Ethernet cable to a device.

```
power inline {never | auto [max <watts (1-16)>]}
```

Parameter	Description
never	Disables Power Over Ethernet on a port.
auto	Enables Power Over Ethernet on a port and gives optional maximum power consumption.

This command can be executed in Interface Configuration Mode.

7.5.3 Show Power

This command shows PoE configuration and status.

```
show power config
show power inline
```

Parameter	Description

config	Disables Power Over Ethernet configuration.
inline	Shows Power Over Ethernet status.

This command can be executed in User or in Privileged Configuration Mode.

8 SECURING ACCESS TO THE UNIT

8.1 Authentication Methods

WEB or CLI access to the device can secured by providing the Username and Password stored either in the local database or on the remote servers (RADIUS or TACACS).

8.1.1 Login Authentication

This command defines the sequence for the authentication with the Username and Password.

```
login authentication [{ radius | tacacs }] [local]
```

Parameter	Description
radius | tacacs	Defines, if the device should try to authenticate the WEB or CLI session by quering the RADIUS ot TACACS server.
local	Defines if the local database should be used for the session authentication. This is the default value. If this paramater is present together with the authentication done by server, the local databease will be used if the RADIUS or TACACS server is not available.

This command can be executed in Global Configuration Mode.

8.2 Local Users

Users that have rights to manage the device are stored in the local database.

8.2.1 Username

This command allows user management in local database.

The no version of this command removes user from the local database

```
username <username> [password [7] <passwd>] [privilege <1-15>]
no username <username>
```

Parameter	Description
password	Password string, the optional parameter “7” tells the system to store the passwords in encrypted format.
privilege	For level 1 only these commands are allowed: Show, Enable, Disable, Exit, Logout, Clear; Level 15 can see all commands.

This command can be executed in Global Configuration Mode.

8.2.2 Set Minimum Password Length

This command defines minimum password length for the users in the local database.

```
set minimum password length <integer (4-128)>
```

Parameter	Description
length	Minimum password length.

This command can be executed in Global Configuration Mode.

8.2.3 Listuser

This command lists all the default and newly created users, along with their permissible mode.

```
listuser
```

Parameter	Description
none	

This command can be executed in Privileged Mode.

8.2.4 Enableuser

This command releases the blocked user specified by the username string.

```
enableuser <username>
```

Parameter	Description
userame	User name to restore

This command can be executed in Global Configuration Mode.

8.3 Authentication with RADIUS

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is used for several reasons:

- RADIUS facilitates centralized user administration(Authentication, Authorization and Accounting).
- RADIUS consistently provides some level of protection against an active attacker.

The following commands configure RADIUS feature in the unit:

8.3.1 RADIUS-Server Host

This command configures the RADIUS client with the parameters (host, timeout, key, retransmit).

The maximum number of radius servers that can be configured is 5.

The no form of the command deletes RADIUS server configuration.

```
radius-server host {ipv4-address | ipv6-address | <dns_host_name>} [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>] [key <secret-key-string>] [primary]

no radius-server host {ipv4-address | ipv6-address | <dns_host_name>} [primary]
```

Parameter	Description
ipv4-address	Configures the IPv4 address of the RADIUS server host.
ipv6-address	Configures the IPv6 address of the RADIUS server host.
dns_host_name	Configures the DNS (Domain Name System) name of the RADIUS server host. This value is a string of maximum size 255.
auth-port	Configures a specific UDP (User Datagram Protocol) destination port on this RADIUS server to be used solely for the authentication requests. This value ranges from 1 to 65535.

acct-port	Configures a specific UDP destination port on this RADIUS to be solely used for accounting requests. This value ranges from 1 to 65535.
timeout	Configures the time period in seconds for which a client waits for a response from the server before re-ransmitting the request. This vlaue ranges 1 to 120 seconds.
retransmit	Configures the maximum number of attempts to be tried by a client to get response from the server for a request. The value number of retransmit attempts ranges between 1 and 254.
key	Configures the per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. This value is a string of maximum size 46. If the key value is not configured, then the default key "RADIUS" will be used.
primary	Sets the RADIUS server as the primary server. Only one server can be configured as the primary server, any existing primary server will be replaced, when the command is executed with this option.

This command can be executed in Global Configuration Mode.

8.3.2 Show RADIUS

This command displays information about RADIUS Server and statistics.

```
show radius server [{<ucast_addr> | <ip6_addr> | <dns_host_name>}]
show radius statistics
```

Parameter	Description
ucast_addr	Displays the related information of the specified unicast address of the RADIUS server host.
ip6_addr	Displays the related information of the specified IPv6 address of the RADIUS server host.
dns_host_name	Displays the name of the RADIUS server host. This value is a string of maximum 255 characters.
statistics	Displays RADIUS Server Statistics.

This command can be executed in Privileged Configuration Mode.

8.4 Authentication with TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. The build-in TACACS Client provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration.
- Uses TCP for transport to ensure reliable delivery.
- Supports inbound authentication, outbound authentication and change password request for the Authentication service.

The following commands configures TACACS feature in the unit:

8.4.1 TACACS-Server Host

This command configures the TACACS server with the parameters (host, timeout, key) and specifies the address of one or more TACACS and the names of the IP host or hosts maintaining a TACACS+ server.

The no form of the command deletes the server entry from the TACACS server table.

```
tacacs-server host {<ipv4-address> | <ipv6-address> | <dns_host_name>} [single-connection]
[port <tcp port (1-65535)>] [timeout <time out in seconds (1-255)>] [key <secret key>]
no tacacs-server host {<ipv4-address> | <ipv6-address> | <dns_host_name>}
```

Parameter	Description
ipv4-address	Configures the IPv4 address of the host.
ipv6-address	Configures the IPv6 address of the host
dns_host_name	Configures the DNS (Domain Name System) name of the TACACS server host. This value is a string of maximum size 255.
single-connection	Allows multiple sessions to be established over a single TCP connection for AAA functionalities.
port	Configures the TCP port number in which the multiple sessions are established. This value ranges from 1 to 65535. Default: 49
timeout	Configures the time period (in seconds) till which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded. This value ranges from 1 to 255 seconds. Default: 5 seconds.
key	Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64.

This command can be executed in Global Configuration Mode.

NOTE: The maximum number of TACACS Servers, that can be configured, is 5.

8.4.2 TACACS Use-Server Address

This command configures the active server address and selects an active server from the list of servers available in the TACACS server table.

The no form of the command disables the configured active server.

```
tacacs use-server address {<ipv4-address> | <ipv6-address> | <dns_host_name>}
no tacacs use-server
```

Parameter	Description
ipv4-address	Configures the IPv4 address of the host.
ipv6-address	Configures the IPv6 address of the host.
dns_host_name	Configures the DNS (Domain Name System) name of the TACACS server host. This value is a string of maximum size 255.

This command can be executed in Global Configuration Mode.

8.4.3 TACACS-Server Retransmit

This command configures the number of servers in the Server-Host list, the TACACS Client tries to connect with, if the Active Server is not defined. The value ranges from 1 to 5.

The no form of the command resets the retransmit value to its default value, that is 2.

```
tacacs-server retransmit <retries (1-5)>
no tacacs-server retransmit
```

Parameter	Description
retries	Number of records in Server-Host list, a TACACS Client tries to query.

This command can be executed in Global Configuration Mode.

8.4.4 Show TACACS

This command displays the server (such as IP address, Single connection, Port and so on) and statistical log information for the build-in TACACS+ client.

```
show tacacs
```

This command can be executed in Privileged EXEC Mode.

9 PORT-BASED AUTHENTICATION WITH 802.1X

802.1X is a client-server-based access control and authentication protocol. It authenticates and authorizes devices attached to a port, thus preventing access from unauthorized clients. The authentication server authenticates each client connected to a port.

Until the client is authenticated, 802.1X access control allows only EAPOL (Extensible Authentication Protocol over LAN) traffic through the port on which the client is connected. When the port connecting the client (Port-Based authentication) is authenticated, normal traffic is allowed through the port.

The 802.1x features can be configured either through CLI or in WEB on Network Security → 802.1x page.

9.1 Dot1x System-Auth-Control

This command enables dot1x in the unit. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames.

The no form of this command disables dot1x in the switch.

```
dot1x system-auth-control
no dot1x system-auth-control
```

Parameter	Description
parameters	none

This command can be executed in Global Configuration Mode.

9.2 AAA Authentication

This command enables the dot1x local authentication or Server based remote authentication method for all ports.

The no form of the command disables authentication in the unit.

```
aaa authentication dot1x default { group {radius | tacacsplus | tacacs+} | local }
no aaa authentication dot1x default
```

Parameter	Description
radius	Configures Radius as the authentication server. Radius offers Authentication, Authorization and Accounting management for computers to access a network.
tacacsplus	Configures TACACS PLUS as the remote authentication server. Tacacs offers Authentication, Authorization and Accounting management for computers to access a network. This is mainly used for backward compatibility.
tacacs+	Configures TACACS+ as the authentication server. This feature has been included to adhere to the Industry Standard CLI syntax.
local	Configures Local authentication as the authentication Mode. It provides authentication based on usernames and password using EAP-MD5 authentication mechanism.

This command can be executed in Global Configuration Mode.

9.3 Dot1x Port-control

This command configures the authenticator port control parameter.

The no form of the command sets the authenticator port control state to force authorized.

```
dot1x port-control {auto|force-authorized|force-unauthorized}
no dot1x port-control
```

Parameter	Description
auto	Configures the 802.1x authentication process in this port. Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch can uniquely identify each client attempting to access the network by the client's MAC address.
force-authorized	Configures the port to allow all the traffic through this port. Disables 802.1X authentication and causes the port to transit to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
force-unauthorized	Configures the port to block all the traffic through this port. Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

This command can be executed in Interface Configuration Mode.

9.4 Dot1x Local-Database

This command configures dot1x authentication server local database with user name and password.

The no form of the command deletes an entry from the dot1x authentication server database.

```
dot1x local-database <username> password <password> permission {allow | deny} [<auth-timeout
(value(1-7200))>] [interface <interface-type> <interface-list>]
no dot1x local-database <username>
```

Parameter	Description
username	Configures the User name for the new entry in the database.
password	Configures the Password for the new entry in the database.
permission	Configures the permission for access for the user on a set of ports. The options are • Allow- Provides access to the user • Deny- Denies access to the user.
auth-timeout	Configures the time in seconds after which the authentication allowed to the user expires. Maximum value is 7200 seconds. When the timeout value is 0, the authenticator uses the re-authentication period of the authenticator port.
interface-type	Configures the interface type for the specified type of interface.
interface-list	Configures the interface list.

This command can be executed in Global Configuration Mode.

9.5 Set NAS-ID

This command sets the dot1x network access server id. Network Access Server Identifier is set in the RADIUS packets sent to the Remote Authentication Server Maximum length of the string is 16.

```
set nas-id <identifier>
```

Parameter	Description
identifier	String, default fsNas1

This command can be executed in Global Configuration Mode.

9.6 Shutdown Dot1x

This command shuts down dot1x feature. By shutting down the dot1x feature, the supplicant-authenticator-authentication server architecture is dissolved. The data transport and authentication are directly governed by the authentication server/server. When shutdown, all resources acquired by dot1x module are released to the system.

The no form of the command starts and enables dot1x.

```
shutdown dot1x
no shutdown dot1x
```

Parameter	Description
none	none

This command can be executed in Global Configuration Mode.

9.7 Dot1x Init-Session

This command initiates or reinitialize dot1x authentication session for the given MAC address of the supplicant. The supplicant requests for access to the protected network. It sends EAPOL(Extensible Authentication Protocol) frames to the authenticator. When the supplicant is authorized by the remote server, the session is initiated.

```
dot1x init-session <supp addr - aa:aa:aa:aa:aa:aa>
dot1x init session-reauth <supp addr - aa:aa:aa:aa:aa:aa >
```

Parameter	Description
supp addr	MAC Address

This command can be executed in Global Configuration Mode.

9.8 Dot1x Default

This command configures dot1x with default values for this port. The previous configurations on this port are reset to the default values.

```
dot1x default
```

Parameter	Description
none	none

This command can be executed in Interface Configuration Mode.

9.9 Dot1x Max-Req

This command sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10.

The no form of the command sets the maximum number of EAP retries to the client to default value.

```
dot1x max-req <count(1-10)>
no dot1x max-req
```

Parameter	Description
count	Count, default value is 2

This command can be executed in Interface Configuration Mode.

9.10 Dot1x Max-Start

This command sets the maximum number of EAPOL retries to the authenticator. The value range is 1 to 65535.

The no form of the command sets the maximum number of EAPOL retries to the authenticator to its default value.

```
dot1x max-start <count(1-65535)>
no dot1x max-start
```

Parameter	Description
count	Count, default value is 3

This command can be executed in Interface Configuration Mode.

9.11 Dot1x Reauthentication

This command enables periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually.

The no form of the command disables periodic re-authentication from authenticator to client.

```
dot1x reauthentication
no dot1x reauthentication
```

Parameter	Description
none	Default Reauthentication is disabled

This command can be executed in Interface Configuration Mode.

9.12 Dot1x Timeout

This command sets the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, starts and stops timer. It provides handlers to respective expired timers.

The no form of the command sets the dot1x timers to the default values.

Only one timer can be configured using this command, that is, the user can configure either the quiet-period or tx-period, but not both.

```
dot1x timeout {quiet-period <value (0-65535)> | {reauth-period | server-timeout | supp-timeout
| tx-period | start-period | held-period | auth-period }<value (1-65535)>}

no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period |
start-period | held-period | auth-period}
```

Parameter	Description
quiet-period	Configures the quiet-period. Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default 60 seconds.
reauth-period	Configures the reath-period. Number of seconds between re-authentication attempts. Default 3600 seconds.
server-timeout	Configures the number of seconds that the switch waits for the retransmission of packets to the authentication server. Default 30 seconds.
supp-timeout	Configures the number of seconds that the switch waits for the retransmission of packets to the client. Default 30 seconds.
tx-period	Configures the number of seconds that the switch waits for a response to an EAP-request/identity frame, from the client before retransmitting the request. Default 30 seconds.
start-period	Configures the number of seconds that the supplicant waits between successive retries to the authenticator. Default 30 seconds.
held-period	Configures the number of seconds that the supplicant waits before trying to acquire the authenticator. Default 60 seconds.
auth-period	Configures the number of seconds that the supplicant waits before timing-out the authenticator. Default 30 seconds.

This command can be executed in Interface Configuration Mode.

9.13 Dot1x Access-Control

This command configures the supplicant access control. This setting is for the application of the Supplicant authorization state when the port is operating as both Supplicant and Authenticator.

The no form of the command sets the access control to inactive.

```
dot1x access-control {active | inactive}
no dot1x access-control
```

Parameter	Description
active	Configures the port to apply both the Supplicant authorization state and Authenticator authorization state.
inactive	Configures the port to use only the Authenticator authorization state to restrict access to the port and not the the Supplicant authorization state

This command can be executed in Interface Configuration Mode.

9.14 Dot1x Control-Direction

This command configures port control direction. The switch port authenticates incoming packets and outgoing packets. The direction can be configured manually by selecting either in or both. By default, the value is both.

The no form of the command sets the authenticator port control direction to both

```
dot1x control-direction {in | both}
no dot1x control-direction
```

Parameter	Description
in	Configures the port to authenticate only the incoming packets.
both	Configures the port to authenticate both incoming and outgoing packets.

This command can be executed in Interface Configuration Mode.

9.15 Dot1x Auth-Mode

This command configures the authentication Mode of a port as either port-based (which is also known as multi-host) or mac-based (which is also known as single-host). Port based authentication has different Modes of authentication. MAC based authentication allows secured mac addresses to pass through the port. Non-secure MAC addresses are dropped.

The no form of the command configures the port authentication Mode to its default values.

To configure the auth Mode of a port as mac-based, port control of the port must be set as auto.

```
dot1x auth-Mode {port-based | mac-based}
no dot1x auth-Mode
```

Parameter	Description
port-based	Configures the port's authentication Mode to Port-based. The port authenticates the host to use the restricted resource. The port state is changed to authorize. The traffic flows through the port without any access restriction till any event that causes the port state to become unauthorized.
mac-based	Configures the port to MAC-based authentication. On receiving tagged/untagged data/control frames from the CFA Module, it checks if the source MAC is present in the Authenticator Session Table and is authorized. • If it is present in the table and is authorized, the result is passed to CFA, which then forwards the frame to the appropriate destination module. • If it is present in the table but not authorized, the CFA Module is intimated and the frame is dropped at the CFA Module. • If neither of the above occurs, the Authenticator will initiate a new authentication session for that source MAC address and return the unauthorized status to the CFA Module, which then drops the frame

This command can be executed in Interface Configuration Mode.

9.16 Dot1x Re-Authenticate

This command initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. This initializes the state machines and sets up the environment for fresh authentication.

Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-auth period). If no interface is specified, re-authentication is initiated on all dot1x ports.

```
dot1x re-authenticate [interface <interface-type><interface-id>]
```

Parameter	Description
interface type	Configures the specified type of interface.

interface id	Configures the specified interface identifier.

This command can be executed in Privileged Mode.

9.17 Show Dot1x

This command displays dot1x information.

```
show dot1x [{ interface <interface-type> <interface-id> | statistics interface <interface-type>
<interface-id> | supplicant-statistics interface <interface-type> <interface-id>|local-database
| mac-info [address <aa.aa.aa.aa.aa.aa>] | mac-statistics [address <aa.aa.aa.aa.aa.aa>] | all}]
```

Parameter	Description
interface type	Configures the specified type of interface.
interface id	Configures the specified interface identifier.
statistics interface	Displays dot1x authenticator port statistics parameters for the switch or the specified interface.
supplicant-statistics	Displays dot1x supplicant statistics parameters for the switch or the specified interface.
local-database	Displays dot1x authentication server database with user name and password.
mac-info	Displays dot1x dot1x information for all MAC session or the specified MAC address.
mac-statistics	Displays dot1x MAC statistic for all MAC session or the specified MAC address.
all	Displays dot1x status for all interfaces

This command can be executed in User or in Privileged Mode.

9.18 Dot1x Clear Statistics

This command clears dot1x statistics information.

```
dot1x clear statistics [{interface <iftype> <ifnum>}][{mac-statistics address <mac_addr>}]
```

Parameter	Description
interface type	Configures the specified type of interface.
interface id	Configures the specified interface identifier.
mac-statistics	Clears dot1x MAC statistics information for all MAC session or the specified MAC address

This command can be executed in Privileged Mode.

10 VLAN CONFIGURATION

Virtual LAN (VLAN) technology, defined in the IEEE 802.1q standard allows enterprises to extend their corporate networks. VLANs group network devices and split them in several broadcast domains. VLANs are secure; they keep the data exchange between the devices in the same VLAN. The inter-VLAN exchange is possible only through routers.

VLAN offers several advantages in compare with traditional LAN:

Performance

VLAN minimizes the possibility of sending the broadcasts and multicasts to unwanted destinations.

Virtual Workgroups

VLAN helps in forming virtual Workgroup environment. Broadcasts and multicasts can be restricted inside Workgroup.

Security

Sensitive data may be periodically broadcasted on a network. VLAN helps keeping it inside defined broadcast domain.

10.1 Static VLANs

10.1.1 VLAN

This command creates VLAN end enters the Config-VLAN Mode, or if this VLAN is already created, this command enters the Config-VLAN Mode for this VLAN.

```
vlan <vlan-id>
```

Parameter	Description
vlan-id	VLAN ID in range from 2 to 4094. VLAN with VID 1 is always present in the unit; VIDs 4095 and 4096 are internally reserved.

The “no” parameter removes VLAN from the system.

```
no vlan <vlan-id>
```

This command can be executed from Global Configuration Mode

10.1.2 Ports

This command manages the VLAN appearance on selected ports. If a port configured as Trunk, any VLAN defined in the system will be a member of this port, unless a forbidden option is set.

For a port working in a Hybrid mode, the VLAN membership must be explicitly defined.

This command has the following syntax:

```
ports [add] ( [<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]) [forbidden <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]]
```

Parameter	Description
add	Appends the new configured ports to the existing member port list of the VLAN.
interface-type	gigabitethernet or gi

0/a-b, 0/c, …	Set the list of all interfaces, Trunk or Hybrid, joing the VLAN. It's a combination of slot and port number separated by the slash. For a single unit the slot number represents always as 0. Example: 0/1, 0/3 0/1-3.
port-channel<a,b,c-d>	Specifies the list of port-channel interfaces. Use comma without space while configuring the list of interfaces. Example: 1,3
forbidden	If a port working mode set as ***Tagged***, all VLANs created in the system are enabled by default. The parameter "forbidden" tells the system that the VLAN with defined VLAN ID is disabled on this port.
all	Deletes all configured member ports from the VLAN. This parameter is available only for "no" form of this command.

Example:

1. Enter the Global Configuration Mode:

```
# configure terminal
```

2. Enter the VLAN configuration Mode (for VLAN with ID = 2):

```
(config)# vlan 2
```

3. Add member ports to the VLAN

```
(config)# ports gigabitethernet 0/4-6 forbidden 0/3
```

Parameter	Description
gigabitethernet 0/4-6	List of interfaces where VLAN with defined ID will work in ***Tagged Mode***. Can be listed with come: 0/1,0/2; as a range: 0/1-3.
forbidden 0/3	List of interfaces where VLAN with defined ID will be disabled.

The "no" parameter removes specified ports from a VLAN:

```
no ports [<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel
<a,b,c-d>] [all] [forbidden ( [<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-
b,0/c,...>] [port-channel <a,b,c-d>] [all] )]
```

This command can be executed in Config-VLAN Mode.

10.1.3 Switchport

This command configures port role as Switchport and sets Access or Native VLAN feature for a port working in Access or Hybrid mode. This command has the following syntax:

```
switchport
switchport access vlan <vlanid (1-4094)>
switchport hybrid native <vlan-id>
switchport mode {access | trunk | hybrid}
switchport priority default <priority value(0-7)>
```

Parameter	Description
switchport	Set the port role as Switchport. The no version of this command sets the port as Router port.
access vlan <vlanid (1-4094)>	Set Access VLAN ID for a port working in Access Mode.
switchport hybrid native <vlan-id>	Set Native VLAN ID for a port working in Hybrid Mode.
switchport mode	Select Port Role between Access, Trunk or Hybrid.

{access | trunk | hybrid}	
switchport priority default <priority value(0-7)>	Set port default priority for incoming untagged packet for ports working in Access or in Hybrid modes.

The “no” version of this command has the following syntax:

```
no switchport
no switchport access vlan
no switchport hybrid native
no switchport mode
no switchport priority default
```

Parameter	Description
no switchport	Set the port as Router port.
no switchport access vlan	Set access VLAN back to default VLAN 1.
no switchport hybrid native	Set Native VLAN ID back to default VLAN 1.
no switchport mode	Select Port Role Back to default: Access.
no switchport priority default	Set port priority for incoming untagged packet for ports working in Access or in Hybrid modes back to default value: 0.

These commands can be executed in Interface Configuration Mode.

10.1.4 Name

This command sets the name of the VLAN. Syntax:

```
name <vlan name string>

no name
```

This command can be executed in Config-VLAN Mode.

10.1.5 VLAN Map-Priority

This command maps a user priority to a traffic class on a port. It has the following syntax:

```
vlan map-priority <priority value(0-7)>  traffic-class <Traffic class value(0-7)>
```

Parameter	Description
priority value(0-7)	The priority determined for the received frame is equivalent to the priority indicated in the received tagged frame.
Traffic class value(0-7)	Configures the traffic class value to which the received frame of specified priority is to be mapped. This value ranges from 0 to 7. Each value represents the concerned traffic. They are: 0 - Best effort. This represents all kinds of non-detrimental traffic that is not sensitive to QoS metrics such as jitter. 1 - Background. This represents bulk transfers and other activities that are permitted on the network without impacting the network usage for users and applications. 2 - Standard (spare traffic). This represents traffic of more importance than background but less importance than excellent load. 3 - Excellent load. This represents the best effort type service that an information services organization should deliver to its most important customers.

	4 - Controlled load. This represents traffic subject to admission control to assure that the traffic is received even when the network is overloaded. 5 - Interactive voice and video. This represents traffic having delay less than 100 milli-seconds. 6 - Internetwork control-Layer 3 network control. This represents traffic having delay less than 10 milli-seconds. 7 - Network control-Layer 2 network control reserved traffic. This represents traffic that demands special treatment based on its requirements and relative importance.

This command can be executed in Interface Configuration Mode.

10.1.6 MAC-Address-Table Static

This command creates MAC Address Entry in the Forwarding Database. This command has the following syntax:

```
mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id> [{recv-port <ifXtype>
<ifnum> }] [interface ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c,
...>] [port-channel <a,b,c-d>][connection-identifier <ucast_mac>] [status { permanent |
deleteOnReset | deleteOnTimeout }]
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id> [{recv-port <ifXtype>
<ifnum>}]
mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id> [recv-port <ifXtype>
<ifnum>] interface ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>]
[port-channel <a,b,c-d>]) [status { permanent | deleteOnReset | deleteOnTimeout }]
no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id > [recv-port <ifXtype>
<ifnum>}]
```

Parameter	Description
unicast <aa:aa:aa:aa:aa:aa>	Configures the static unicast destination MAC Address.
multicast <aa:aa:aa:aa:aa:aa>	Configures the static multicast destination MAC Address.
vlan <vlan-id>	Configures VLAN ID. VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094
recv-port <ifXtype> <ifnum>	Configures receive port details. Only packets received on this ports are processed. The details are: ifXtype is gigabitethernet or gi, or portchannel. Ifnum is interface number in format slot number, port number serparated by the slash.
connection-identifier<ucast_mac>	Associates backbone MAC address of peer backbone edge bridge with customer MAC address that can be reached through the bridge.
status	Specifies the status of the MAC Address entry: • permanent: Entry remains even after the next reset of the unit. This is the default value. • deleteOnReset: Entry remains until the next reset of the unit. • deleteOnTimeout: Entry remains until it is aged out.
no	The “no” version of the command removes the entry from the Forwarding Database.

This command can be executed in the Global Configuration Mode. The MAC-Address Table can be shown with `show mac-address-table` command.

10.1.7 Show VLAN

This command displays the VLAN-related information. It has the following syntax:

```
show vlan [brief | id <vlan-range> | summary | ascending]
show vlan port config [{port <interface-type> <interface-id>}]
show vlan statistics [vlan <vlan-range>]
show vlan traffic-classes [{port <interface-type> <interface-id>}]
```

Parameter	Description
brief	Show brief information about VLANs
id <vlan-range>	Show information about defined VLAN
summary	Show number of VLANs in the system
ascending	Show VLAN-related information in ascending order
port config	Show Port-related information
statistics	Show statistics information
traffic-classes	Shows user priority and traffic class mapping information

This command can be executed in Privileged EXEC Mode.

10.2 GVRP

GVRP uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in a LAN. This information allows GVRP aware devices to dynamically establish and update the information about the existence of the VLANs in a topology. The GVRP registers the created VLANs with GARP and de-registers the deleted VLANs from the GARP.

For the successful dynamic VLAN registration on a peer, one of the units in the LAN must have static VLAN configuration.

10.2.1 Shutdown GARP

This command shuts down the GARP module in the unit on all ports and releases all resources used for the GARP module.

The no form of the command starts and enables the GARP module in the unit on all ports. GVRP is enabled explicitly, once the disabled GARP is enabled.

GARP is used to synchronize attribute information between the bridges in the LAN. It allows registering and de-registering attribute values, which are disseminated into the backbone of the GARP participants It has the following syntax:

```
shutdown garp
no shutdown garp
```

This command can be executed in Global Configuration Mode.

10.2.2 Set GVRP

This command globally enables or disables GVRP service on all ports of the system. It has the following syntax:

```
set gvrp { enable | disable }
```

Parameter	Description
enable	Enables GVRP feature on all ports of the system.
disable	Disables the GVRP feature on all ports of the system

This command can be executed in Global Configuration Mode.

10.2.3 Set Port GVRP

This command enables or disables GVRP feature on the specified interface. It has the following syntax:

```
set port gvrp <interface-type> <interface-id> { enable | disable }
```

Parameter	Description
interface-type	gigabitethernet or gi
interface-id	Defines the interface, where GARP feature should be configured. This value is a combination of slot number and port number separated by a slash.
enable	Enables GVRP feature on the specified port of the system.
disable	Disables the GVRP feature on the specified port of the system.

This command can be executed in Global Configuration Mode.

10.2.4 VLAN Restricted

This command configures the restricted VLAN registration feature in a port. This feature configures the dynamic registration of VLAN. It has the following syntax:

```
vlan restricted {enable | disable}
```

Parameter	Description
enable	Enables restricted VLAN registration feature in the port. The creation or modification of a dynamic VLAN entry is permitted only for VLANs for which static VLAN registration entries exist.
disable	Disables restricted VLAN registration feature in the port. The creation or modification of a dynamic VLAN entry is permitted for all VLANs. This is the default setting.

This command can be executed in Interface Configuration Mode.

10.3 MRP

MRP (Multiple Registration Protocol) is a simple, distributed, and many-to-many protocol. MRP supports efficient, reliable, and rapid declaration and registration of the attributes by multiple participants on shared media.

MRP also incorporates optimizations to speed attribute declarations and withdrawals on point-to-point media.

10.3.1 Shutdown MRP

This command shuts down MRP module in the system on all ports. All allocated memory is released, when the MRP module is shutdown. MRP can be shut down only when none of the MRP applications MVRP (Multiple VLAN Registration Protocol) and MMRP (Multiple MAC Registration Protocol) are enabled. This command has the following syntax:

```
shutdown mrp
no shutdown mrp
```

GARP and GVRP services should be in shutdown state before enabling MRP module.

This command can be executed in Global Configuration Mode.

10.3.2 Set MVRP | MMRP

This command configures the MVRP / MMRP feature in the unit. This command has the following syntax:

```
set { mvrp | mmrp } { enable | disable }
```

Parameter	Description
mvrp	Configures Multiple VLAN Registration Protocol feature.
mmrp	Configures Multiple MAC Registration Protocol feature.
enable	Enables the MVRP / MMRP application in the switch. Default: Enabled if MRP is enabled.
disable	Disables the MVRP / MMRP application in the switch.

This command can be executed in Global Configuration Mode.

10.3.3 Set Port MVRP | MMRP <Parameters>

This command configures the MVRP / MMRP application on the port. It has the following syntax:

```
set port { mvrp | mmrp } <interface-type> <interface-id> { enable | disable }
set port { mrp | mvrp } <interface-type> <interface-id> periodictimer { enable | disable }
set port mrp <interface-type> <interface-id> participant { full-participant | applicant-only }
set port mmrp { mac | service-requirement } <interface-type> <interface-id> applicant { normal
| non-participant }
set port mvrp <interface-type> <interface-id> applicant { normal | non-participant | active }
set port mrp <interface-type> <interface-id> timer { join | leave | leaveall } <time in centi
seconds>
set port mvrp <interface-type> <interface-id> registration {normal | fixed | forbidden}
```

Parameter	Description
mvrp	Configures Multiple VLAN Registration Protocol feature. Default: Enabled if MRP is enabled.
mmrp	Configures Multiple MAC Registration Protocol feature. Default: Enabled if MRP is enabled.
interface-type	gigabitethernet or gi
interface-id	Defines the interface, where MVRP / MMRP feature should be configured. This value is a combination of slot number and port number separated by a slash.
enable	Enables the MVRP / MMRP application in the switch, or activates a parameter.

disable	Disables the MVRP / MMRP application in the switch, or activates a parameter.
periodictimer	Enables or disables periodic timer on the port. If enabled, the port will generate transmission events on a periodic basis, against all applicant state machines that are associated with the port. Default: periodic timer is Disabled.
participant full-participant	Configures the participant type that implements the complete applicant state machine and the registrar state machine for each attribute declared, registered or tracked, together with a single instance of the LeaveAll state machine and the periodic state machine. This is the Default value.
participant applicant-only	Configures the participant type that implements the applicant state machine with omission of certain states and actions (as specified by Table 10-3 in IEEE Standard 802.1ak-2007), for each attribute declared or tracked, together with a single instance of the periodic state machine. LeaveAll state machine and registrar state machine are not applicable for this participant type.
mmrp mac	Configures the MAC Vector Attribute type of MMRP application.
mmrp service-requirement	Configures the Service Requirement Vector Attribute type of MMRP application.
mmrp applicant normal	Indicates that the applicant participates normally in MRPDU exchanges.
mmrp applicant non-participant	Indicates that the MRP participant does not transmit any MRPDUs.
mvrp applicant normal	Indicates that the applicant participates normally in MRPDU exchanges. This is the default value.
mvrp applicant non-participant	Indicates that the MRP participant does not transmit any MRPDUs.
mvrp applicant active	Allows to send VLAN declarations, when the port is in the blocking state.
mrp timer join	Configures MRP Join time. This time defines the time interval (in centi-seconds) between transmit opportunities. This value ranges from 20 to10000000 centi-seconds. Default value is 20 centi-seconds.
mrp timer leave	Configures MRP Leave time. This defines the time (in centi-seconds) that the Registrar state machine should wait in LV state before transiting to an MT state. This value ranges from 60 to10000000 centi-seconds. Default value is 60 centi-seconds.
mrp timer leaveall	Configures MRP LeaveAll time. This defines the time interval (in centi-seconds) in which all the leaveall message is generated. This value ranges from 1000 to10000000 centi-seconds. Default value 1000 centi-seconds.
mvrp registration normal	Configures the type of the registrar admin control as normal. If registrar admin control of a port is configured as normal, then the registrar state machine responds to incoming messages. This is the default value.
mvrp registration fixed	Configures the type of the registrar admin control as fixed. If registrar admin control of a port is configured as fixed, then the registrar state machine ignores all MRP messages. All the learnt attributes are aged out through the LeaveAll mechanism.
mvrp registration forbidden	Configures the type of the registrar admin control as forbidden. If registrar admin control of a port is configured as forbidden, then the registrar state machine ignores all MRP messages. All the learnt attributes are removed immediately.

This command can be executed in Global Configuration Mode.

10.3.4 Set VLAN | MAC Notify Failed-Registration

This command enables / disables the trap for notifying VLAN / MAC registration failure. It has the following syntax:

```
set { vlan | mac } notify failed-registration { enable | disable }
```

Parameter	Description
vlan	Configures VLAN registration failures. This specifies the administrative trap control status requested by management for notifying MVRP registration failures.
mac	Configures MAC registration failures. This specifies the administrative trap control status requested by management for notifying MMRP registration failures.
enable	Enables trap notification.
disable	Disables trap notification. This is the default value.

This command can be executed in the Global Configuration Mode.

10.3.5 MRP VLAN Restricted

This command enables / disables the restricted VLAN registration on the port. If restricted VLAN registration is enabled, then the creation of a new dynamic VLAN entry is permitted, only if a static VLAN registration entry is present in the system. This command has the following syntax:

```
mrp vlan restricted { enable | disable }
```

Parameter	Description
enable	Enables restricted VLAN registration feature.
disable	Disables restricted VLAN registration feature. Ths is the default setting.

This command can be executed in the Interface Configuration Mode.

10.3.6 MRP MAC-Address Restricted

This command enables / disables restricted MAC address registration on the port. If restricted MAC Address registration is enabled, then the creation or modification of Dynamic MAC Address Registration entry as a result of MMRP exchanges on the port is permitted, only if there is a static MAC Address entry is present on the interface. This command has the following syntax:

```
mrp mac-address restricted { enable | disable }
```

Parameter	Description
enable	Enables restricted MAC Address registration feature.
disable	Disables restricted MAC Addres registration feature. Ths is the default setting.

This command can be executed in the Interface Configuration Mode.

10.3.7 Show MRP | MVRP | MMRP

This command displays various MRP, MVRP or MMRP settings. It has the following syntax:

```
show { mrp | mvrp | mmrp } configuration [{port <interface-type> <interface-id>]
show { mrp | mvrp | mmrp } statistics [{port <interface-type> <interface-id>]
show mvrp machines [vlan <vlan-id>] [{port <interface-type> <interface-id>]
show mvrp machines [vlan <vlan-id>] [{port <interface-type> <interface-id>]
```

```
show mrp timer [{ port <interface-type> <interface-id>]
```

Parameter	Description
mrp	Displays Multiple Registration Protocol applications (that is, both MVRP and MMRP applications) configuration details.
mvrp	Displays Multiple VLAN Registration Protocol application configuration details.
mmrp	Displays Multiple MAC Registration Protocol application configuration details.
interface-type	gigabitethernet or gi
interface-id	Defines the interface, where MVRP / MMRP feature should be configured. This value is a combination of slot number and port number separated by a slash.
configuration	Tels the system to display configuration information.
statistics	Tels the system to display statistic information.
machines	Shows state-machines information.
timer	Shows timer information

This command can be executed in Privileged EXEC Mode.

11 SPANNING TREE

STP (Spanning-Tree Protocol) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all switches in an extended network, forcing redundant paths into a standby or blocked state.

For an Ethernet network to function properly, only one active path should exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP logically breaks such loops and prevents looping traffic from clogging the network. The dynamic control of the topology provides continued network operation in the presence of redundant or unintended looping paths.

The Spanning Tree can be configured either through CLI or in WEB on Network Redundancy → Spanning Tree Page.

11.1 Common Configuration

11.1.1 Spanning-Tree

This command enables the spanning tree operation in the switch for the selected spanning tree Mode.

The no form of this command disables the spanning tree operation in the switch. The spanning tree operation is automatically enabled in the switch, once the spanning tree Mode is changed.

```
spanning-tree
no spanning-tree
```

These commands can be executed in Global Configuration Mode.

11.1.2 Spanning-Tree Mode

This command sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the unit. The current selected type of spanning tree is enabled, and the existing spanning tree type is disabled in the switch.

The no version of this command restores default value.

```
spanning-tree mode {mst | rst | pvrst}
no spanning-tree mode
```

Parameter	Description
mst	Configures the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. This is default mode.
rst	Configures the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN.
pvrst	Configures the switch to execute PVRST+ for preventing undesirable loops. PVRST+ is an enhancement of RSTP which works in combination with VLAN to provide better control over traffic in the network. The Mode cannot be set as pvrst. The pvrst can be set as the spanning tree Mode, only if the GVRP feature is disabled.

This command can be executed in Global Configuration Mode.

11.1.3 Spanning-Tree Compatibility

This command sets the STP compatibility version in the switch for all ports.

The no form of this command sets the STP compatibility version to its default value. The STP compatibility version is changed to its default value even if the spanning tree Mode is changed.

The compatibility version allows the switch to temporarily operate (that is, till this configuration is reset manually) in other STP version even though the spanning tree Mode is set as some other version. This configuration is useful during cases where spanning tree Mode itself is not required to be changed.

```
spanning-tree compatibility {stp | rst | mst}
no spanning-tree compatibility
```

Parameter	Description
stp	Configures the switch to execute spanning tree operation as specified in IEEE 802.1D.
rst	Configures the switch to execute spanning tree operation as specified in IEEE 802.1w.
mst	Configures the switch to execute spanning tree operation as specified in IEEE 802.1s. The STP compatibility version cannot be set as mst, if the spanning tree Mode is set as rst.

This command can be executed in Global Configuration Mode.

11.1.4 Spanning-Tree Priority

This command configures the priority value that is assigned to the unit.

The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree Mode is changed.

In RSTP, this value is used during the election of root. In MSTP, this value is used during the election of CIST root, CIST regional root and IST root.

```
spanning-tree [mst <instance-id>] priority <value(0-61440)>
no spanning-tree [mst <instance-id(1-64)>] priority
```

Parameter	Description
mst <instance-id>	Configures the ID of MSTP instance already created in the switch. This value ranges from 1 to 64. This option is applicable, only if the spanning tree Mode is set as mst.
priority <value(0-61440)>	Configures the priority value for the switch and for the MSTI, in RSTP and MSTP respectively. This value ranges from 0 to 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.

This command can be executed in Global Configuration Mode.

11.1.5 Spanning-Tree Pathcost Dynamic

This command enables dynamic pathcost calculation feature in the switch.

The no form of this command disables dynamic pathcost calculation feature in the switch. The dynamic pathcost calculation feature is disabled, even if the spanning tree Mode is changed.

The path cost of the port / MSTI is dynamically calculated. This feature is applied only for the ports that are not shutdown during the execution of STP. The calculated path cost is not changed based on the operational status of the port / for a MSTI, once calculated. The manually assigned / already calculated path cost is used even if the dynamic pathcost calculation feature is enabled in the switch.

```
spanning-tree pathcost dynamic [lag-speed]
no spanning-tree pathcost dynamic [lag-speed]
```

Parameter	Description
lag-speed	Calculates the path cost for change in speed of the port. This feature is used for LA ports whose speed changes due to addition or deletion of ports from the port channel. The manually assigned path cost is used even if the lag speed feature is enabled in the switch, if the path cost is assigned manually. The lag speed feature can be enabled, only after enabling the dynamic pathcost calculation feature.

This command can be executed in Global Configuration Mode.

11.1.6 Spanning-Tree Portfast Bpduguard Default

This command enables BPDU Guard functionality globally on all edge ports. BPDU guard puts an interface in the error-disabled state when it receives a bridge protocol data unit. Portfast specifies that port has only hosts connected and hence change to forwarding state rapidly.

The no form of the command disables BPDU Guard functionality globally on all edge ports.

```
spanning-tree portfast bpduguard default
no spanning-tree portfast bpduguard default
```

This command can be executed in Global Configuration Mode.

11.1.7 Spanning-Tree Transmit Hold-Count

This command sets the transmit hold-count value for the switch, where the value is a counter that is used to limit the maximum transmission rate of the switch and to avoid flooding. This value specifies the maximum number of packets that can be sent in a given hello time interval. This value ranges from 1 to 10.

The no form of this command sets the transmit hold-count to its default value. The transmit hold-count is changed to its default value even if the spanning tree Mode is changed.

```
spanning-tree transmit hold-count <value (1-10)>
no spanning-tree transmit hold-count
```

Parameter	Description
value	From 1 to 10. Defaults are: • For MST: 6 • For RST or PVRST: 3

This command can be executed in Global Configuration Mode.

11.1.8 Spanning-Tree Timers

This command sets the spanning tree timers such as hello time used for controlling the transmission of BPDUs during the computation of loop free topology.

The no form of this command resets the spanning tree timers to its default values. The spanning tree timers are reset to its default value, even if the spanning tree Mode is changed.

```
spanning-tree {forward-time <seconds(4-30)> | hello-time <seconds(1-2)> | max-age <seconds(6-40)>}
no spanning-tree { forward-time | hello-time | max-age }
```

Parameter	Description
forward-time	Configures the number of seconds, a port waits before changing from the blocking state to the forwarding state. This value ranges from 4 to 30 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). Default: 15 seconds.
hello-time	Configures the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value should be either 1 or 2 seconds. This value is configured on per-port basis for MSTP and is configured globally for RSTP. Default: 2 seconds.
max-age	Configures the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval. This value ranges from 6 to 40 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). Default: 20 Seconds.

This command can be executed in Global Configuration Mode.

11.1.9 Spanning Tree Properties of an Interface

This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP/MSTP Mode.

The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree Mode is changed.

```
spanning-tree [{cost <value(0-200000000)> | disable | link-type {point-to-point | shared}|
portfast | port-priority <value(0-240)>}]
no spanning-tree [{cost | disable | link-type | portfast | port-priority}]
```

Parameter	Description
cost	Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges from 1 to 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. This configuration is not supported for the spanning tree Mode pvrst.
disable	Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.
link-type	Configures the link status of the LAN segment attached to the port. The options available are: • point-to-point – The port is treated as if it is connected to a point-to-point link. • shared - The port is treated as if it is using a shared media connection.
portfast	Configures the portfast feature in the port. This feature specifies that the port is connected to only one hosts and hence can rapidly transit to forwarding. This feature can cause temporary bridging loops, if hubs,

	concentrators, switches, bridges and so on are connected to this port. This feature takes effect only when the interface is shutdown.
port-priority	Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges from 0 to 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. This configuration is not supported for the spanning tree Mode pvrst.

This command can be executed in Physical Interface Configuration Mode.

11.1.10 Spanning-Tree Auto-Edge

This command enables automatic detection of Edge port parameter of an interface.

The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree Mode is changed.

Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received.

```
spanning-tree auto-edge
no spanning-tree auto-edge
```

This command can be executed in Physical Interface Configuration Mode.

11.1.11 Spanning-Tree BPDU Receive | Transmit

These commands configure the BPDU transmission and reception status of a port. BPDUs are used to carry bridge related information that is used during spanning tree operation.

The status is reset to its default value, once the spanning tree Mode is changed.

```
spanning-tree bpdu-transmit {enabled | disabled}
spanning-tree bpdu-receive {enabled | disabled}
```

Parameter	Description
enable	Allows normal processing of BPDUs received on a port; allows egress BPDUs. This is the default value.
disable	Discard incoming BPDU; don't send BPDUs.

This command can be executed in Physical Interface Configuration Mode.

11.1.12 Spanning-Tree Bpduguard

This command configures the status of BPDU guard feature in an interface.

The BPDU guard feature disables the port and puts the port in error-disabled state on receiving BPDU, if the Portfast feature is enabled on the port. This feature prevents the devices connected to the port from participating in STP operation. Once disabled, the port can be enabled only manually.

The no form of this command disables the BPDU guard feature.

```
spanning-tree bpduguard {disable | enable [ { admin-down | disable-discarding } ] | none}
no spanning-tree bpduguard
```

Parameter	Description
disable	Disables BPDU guard feature in the interface and the port state is maintained till it is manually made up.
enable	Enables BPDU guard feature in the interface to prevent temporary loops and moves the port to disabled discarding state when BPDU is received on this port. • admin-down - Disables the port and puts the port in error-disabled state on receiving BPDU • disable-discarding - Disables spanning-tree on the port
none	Removes BPDU guard on the specified interface. Global BPDU guard configuration takes effect if this port is edge port.

This command can be executed in Physical Interface Configuration Mode.

11.1.13 Spanning-Tree Guard

This command configures the various guard features such as root guard, on a port.

The no form of this command resets the guard feature to its default value.

Root Guard implementation in PVRST is applicable only for trunk ports.

This parameter can be configured only for Point-to-point links. Loop guard feature is not supported for shared links.

```
spanning-tree guard {root | none | loop}
no spanning-tree guard
```

Parameter	Description
root	Enables root guard feature on the port. This feature prevents the port from becoming root port or blocked port. The port changes to the root-inconsistent state, if the port receives superior BPDUs. The port automatically reverts back to forwarding state, once the superior BPDUs are not received.
none	Disables both root and loop guard features on the port. This is the default value.
loop	Enables loop guard feature on the port. This feature changes the port to an inconsistent state if no BPDUs are received. Thus isolating the failure and letting spanning tree converge to a stable topology until the port starts receiving BPDUs again.

This command can be executed in Physical Interface Configuration Mode.

11.1.14 Spanning-Tree Loop-Guard

This command enables the loop guard feature in a port.

This feature prevents the alternative or root ports from becoming designated ports due to failure in a unidirectional link. This feature is useful when the neighbour bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic.

The no form of this command disables the loop guard feature in the port. The loop guard feature is disabled, even if the spanning tree Mode is changed.

```
spanning-tree loop-guard
no spanning-tree loop-guard
```

This command can be executed in Physical Interface Configuration Mode.

11.1.15 Spanning-Tree Mode Dot1w

This command enables or disables the bridge to send agreement PDU in accordance with 802.1W (dot1w).

```
spanning-tree mode dot1w {enable | disable}
```

Parameter	Description
enable	Enables the bridge to send agreement pdu in accordance with 802.1W.
disable	Disables the bridge to send agreement pdu in accordance with 802.1W. This is the default value.

This command can be executed in Physical Interface Configuration Mode.

11.1.16 Spanning-Tree Restricted

These commands enable restricted Spanning Tree feature on a port. The no version of these commands restores the default value.

```
spanning-tree restricted-role
no spanning-tree restricted-role
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Parameter	Description
role	The restricted role feature blocks the port from being selected as a root port even if it has the best spanning tree priority vector. This port is selected as an alternate port after the root port is selected. This feature allows you to block switches external to a core region of the network from influencing the spanning tree active topology. The blocking of port from being selected as a root port can cause lack of spanning tree connectivity.
tcn	The restricted TCN feature blocks the port from propagating the received topology change notifications and topology changes to other ports. This feature allows you to block switches external to a core region of the network from causing address flushing in the region. The blocking of port can cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information.

This command can be executed in Physical Interface Configuration Mode.

11.1.17 Show Spanning-Tree

This command displays various Spanning Tree Parameters.

```
show spanning-tree [{summary | blockedports | pathcost method}]
show spanning-tree active [detail]
show spanning-tree bridge [{address | forward-time | hello-time | id | max-age | protocol |
priority | detail}]
show spanning-tree detail
show spanning-tree interface <ifXtype> <ifnum> bpduguard
show spanning-tree interface <ifXtype> <ifnum> inconsistency
show spanning-tree interface <interface-type> <interface-id> [{cost | encapsulationtype |
priority | portfast | rootcost |restricted-role | restricted-tcn | state | stats | detail }]
```

```
show spanning-tree mst [<instance-id(1-64 or 4094)>] [detail]
show spanning-tree mst [<instance-id(1-64 or 4094)>] interface <interface-type> <interface-id>
[{ stats | hello-time | detail }]
show spanning-tree mst configuration
show spanning-tree performance-data [interface <interface-type> <interface-id> [instance
<instance-id>]]
show spanning-tree root [{address | cost | forward-time | id | max-age | port | priority |
detail}]
show spanning-tree vlan <vlan-id> [{blockedports | pathcost-method | summary}]
show spanning-tree vlan <vlan-id> active [detail]
show spanning-tree vlan <vlan-id> bridge [{address | detail | forward-time | hello-time | id |
max-age | priority [system-id] | protocol}]
show spanning-tree vlan <vlan-id> detail [active]
show spanning-tree vlan <vlan-id> interface <ifXtype> <ifnum> [{ cost | detail | priority |
rootcost | state | stats }]
show spanning-tree vlan <vlan-id> root [{address | cost | detail | forward-time | hello-time |
id | max-age | port | priority [system-id]}]
```

Parameter	Description
summary	Displays the currently used STP, applied path cost method and port details such as port ID, port role, port state and port status. This option cannot be executed in the PVRST Mode.
blockedports	Displays the list of ports in blocked state and the total number of blocked ports. This option cannot be executed in the PVRST Mode.
pathcost method	Displays the port pathcost method configured for the switch.
redundancy	Displays the port role and port state, and dumps the STP port related information.
detail	This command displays detailed spanning tree related information of the switch and all ports enabled in the switch.
cost	Displays the cost of the port or instances assigned to that port. This option cannot be executed in the PVRST Mode.
encapsulationtype	Displays the encapsulation type used in the interface.
priority	Displays the priority of the port or instances assigned to that port. This option cannot be executed in the PVRST Mode.
portfast	Displays the status of the portfast feature for the port or instances assigned to that port.
rootcost	Displays the root cost of the port or instances assigned to that port. The root cost defines the pathcost to reach the root bridge. This option cannot be executed in the PVRST Mode.
restricted-role	Displays the status of the restricted role feature for the port. This option cannot be executed in the PVRST Mode.
restricted-tcn	Displays the status of the restricted TCN feature for the port. This option cannot be executed in the PVRST Mode.
state	Displays the state of the port. This option cannot be executed in the PVRST Mode.
stats	Displays the port level spanning tree statistics information. This option cannot be executed in the PVRST Mode.
root	This command displays the spanning tree root information. The information contain root ID, root path cost, maximum age time, forward delay time and root port, for the RSTP. The information also contains the instance ID for MSTP.
bridge	This command displays the spanning tree bridge information. The information contain bridge ID, hello time, maximum age time, forward delay

	time and protocol enabled, for the RSTP. The information also contains the instance ID for MSTP.
mst	This command displays multiple spanning tree information for all MSTIs in the switch.
mst configuration	This command displays multiple spanning tree instance related information. This information contains the MST region name, MST region revision, and a list containing MSTI IDs and VLAN IDs mapped to the corresponding MSTI.
mst port	This command displays multiple spanning tree port specific information for the specified port. This information contains interface ID, edge port status, port link type, port hello time, BPDUs sent and received on the port, and instance related details. The instance details contain MSTI ID, MSTI role, MSTI status, MSTI cost and MSTI priority.
vlan	This command displays PVRST related information for the specified VLAN.

This command can be executed in User or in Privileged Configuration Mode.

11.1.18 MSTP Configuration

11.1.19 Spanning-Tree MST

This command creates an MST instance in the unit.

The no version of this command removes MST instance from the unit.

```
spanning-tree mst {instance-id <instance-id(1-64)>} root {primary | secondary}
no spanning-tree mst {instance-id <instance-id(1-64)>} root
```

Parameter	Description
instance-id	Configures the ID of MSTP instance already created in the switch. This value ranges from 1 to 64. This option is applicable, only if the spanning tree Mode is set as mst.
primary	Sets high enough priority (low value) for the switch so that the switch can be made as the bridge root of the spanning-tree instance. The priority value is set as 24576.
secondary	Sets the switch as a secondary root, if the primary root fails. The priority value is set as 28672.

This command can be executed in Global Configuration Mode.

11.1.20 Spanning-Tree MST Configuration

This command enters the MST Configuration mode

```
(config)# spanning-tree mst configuration
(config-mst)#
```

This command can be executed in Global Configuration Mode.

11.1.21 Spanning-Tree Properties of an Interface for MSTP

This command configures the port related spanning tree information for a specified MSTI in a port.

The no form of this command resets the spanning tree information of a port to its default value.

```
spanning-tree mst <instance-id(1-64)> { cost <value(1-200000000)>| port-priority <value(0-240)>
| disable }
```

```
no spanning-tree {mst <instance-id(1-64)>} {cost|port-priority | disable}
```

Parameter	Description
instance-id	Configures the ID of MSTP instance already created in the switch.This value ranges from 1 to 64.
cost	Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges from 1 to 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAG speed feature is enabled.
port-priority	Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges from 0 to 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. The MSTP puts the interface with lowest number in forwarding state and blocks all other interfaces, if all interfaces have the same priority value.
disable	Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.

This command can be executed in Physical Interface Configuration Mode.

11.1.22 Spanning-Tree MST Hello-Time

This command configures the spanning tree hello time.

The no form of this command resets the hello time to its default value.

The hello time represents the time interval (in seconds) between two successive configuration BPDUs generated by the switch on the port. This value is either 1 or 2 seconds. This value is applied to all active MSTIs.

```
spanning-tree mst hello-time<value(1-2)>
no spanning-tree mst hello-time
```

Parameter	Description
value	1 or 2 seconds. Default: 2 seconds.

This command can be executed in Physical Interface Configuration Mode.

11.1.23 Instance

This command creates an MST instance and maps it to VLANs.

The no form of this command deletes the instance / un-maps specific VLANs from the MST instance.

```
instance <instance-id(1-64)> vlan <vlan-range>
no instance <instance-id (1-64)> [vlan <vlan-range>]
```

Parameter	Description
instance-id	Configures the ID of MSTP instance to be created / deleted and mapped with / un-mapped from VLAN. This value ranges from 1 to 64.
vlan	Configures a VLAN ID or list of VLAN IDs that should be mapped with / un-mapped from the specified MST instance. For Example, the value is provided as 4000-4010 to represent the list of VLANs IDs from 4000 to 4010.

This command can be executed in MST Configuration Mode.

11.1.24 Name

This command configures the name for the MST region.

The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances.

The no form of this command resets the name to its default value.

```
name <string(optional max Length)>
no name
```

This command can be executed in MST Configuration Mode.

11.1.25 Revision

This command configures the revision number for the MST region. This value ranges from 0 to 65535.

The no form of this command resets the revision number to its default value.

```
revision <value(0-65535)>
no revision
```

This command can be executed in MST Configuration Mode.

11.2 PVST+ Configuration

11.2.1 Spanning-Tree VLAN

This command configures spanning tree related information on a per VLAN basis.

The no form of this command resets the spanning tree related information to its default values.

The values configured for the spanning tree forward timers should satisfy the following conditions:

2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)

```
spanning-tree vlan <vlan-id> {forward-time <seconds(4-30)> | hello-time <seconds(1-10)> | max-
age <seconds(6-40)> | hold-count <integer(1-10)> | brg-priority <integer(0-61440)> | root
{primary | secondary}}
no spanning-tree vlan <vlan-id> {forward-time <seconds(4-30)> | hello-time <seconds(1-10)> |
max-age <seconds(6-40)> | hold-count <integer(1-10)> | brg-priority <integer(0-61440)> | root
{primary | secondary}}
```

Parameter	Description
vlan-id	VLAN ID in range from 1 to 4094
forward-time	Configures the number of seconds, a port waits before changing from the listening and learning states to the forwarding state. This value ranges from 4 to 30 seconds. Default: 15 seconds.
hello-time	Configures the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value ranges from 1 to 10 seconds. Default: 2 seconds.
max-age	Configures the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval. This value ranges from 6 to 40 seconds. Default: 20 seconds.

hold-count	Configures the maximum number of packets that can be sent in a given hello time interval. This value is used to limit the maximum transmission rate of the switch and to avoid flooding. This value ranges from 1 to 10. Default: 3
brg-priority	Configures the bridge priority to be assigned for the specified VLAN. This value ranges from 0 to 61440. The value should be set in increments of 4096, that is, the value can be set as 0, 4096, 8192, 12288 and so on. Default: 32868 + VLAN ID.
root {primary | secondary}	Configures the root type for the given vlan interface. The options are: • primary - Configures the switch to become root for a given VLAN. The priority of the switch is lowered until it becomes root. • secondary - Configures the switch to become backup root for a given VLAN. The priority of the switch is lowered until it becomes one priority higher than the root, so it can become root if the current root fails.

This command can be executed in Global Configuration Mode.

11.2.2 Spanning-Tree ENCAP

This command configures the encapsulation type to be used in an interface. The encapsulation defines the VLAN services available and identifies / tags frames transmitted between switches.

The no form of this command resets the encapsulation type to its default value.

```
spanning-tree encap {dot1q | ISL}
no spanning-tree encap
```

Parameter	Description
dot1q	Configures the encapsulation type as dot1Q. The port sends BPDUs for the native VLAN as normal IEEE RSTP BPDUs. The port sends BPDUs for other VLANs with proprietary tunneled address. The PVRST unaware bridge considers these BPDUs as data packets and forward them through VLAN. This option is automatically set for the port, if the port is configured as access port. This is the default value.
ISL	Configures the encapsulation type as ISL. The port sends BPDUs for all VLANs as normal RSTP BPDUs (including the IEEE Ethernet header) encapsulated within an additional proprietary ISL Ethernet header that contains the VLAN ID. This option can set only for the port that is configured as trunk port

This command can be executed in Global Configuration Mode.

11.2.3 Spanning Tree VLAN Interface Configuration Mode.

These commands configure various parameters of PVRST on a port for specified VLAN. The no version of these commands restores default values.

```
spanning-tree vlan <vlan-id> cost <cost(0-200000000)>
spanning-tree vlan <vlan-id> port-priority <priority(0-240)>
spanning-tree vlan <vlan-id> status {disable | enable}
no spanning-tree vlan <vlan-id/vfi_id> port-priority
no spanning-tree vlan <vlan-id/vfi_id> cost
```

Parameter	Description
vlan	VLAN ID

cost	Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges from 1 to 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled.
port-priority	Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges from 0 to 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48 and so on.
status	disable - Disables the PVRST operation on the port for the specified VLAN ID. enable - Enables the PVRST operation on the port for the specified VLAN ID.

This command can be executed in Physical Interface Configuration Mode.

12 LLDP

LLDP (Link Layer Discovery Protocol) supports a set of attributes that it uses to discover the neighbour devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbours.

The unit supports these mandatory basic management TLVs:

- Port description TLV
- System name TLV
- System description
- System capabilities TLV
- Management address TLV
- Port VLAN ID TLV ((IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV(IEEE 802.3 organizationally specific TLVs)

The LLDP realisation conforms to IEEE 802.1AB-2005 standard. The LLDP allows systems on an Ethernet LAN to advertise their key capabilities and to learn about the key capabilities of other systems on the same Ethernet LAN.

The LLDP-related parameters can be configured either through CLI or in WEB on the General Settings → Network Discovery Page.

12.1 Shutdown LLDP

This command shuts down all the ports in the LLDP and releases all the allocated memory.

The no form of the command enables all the ports by allocating the required resources in the LLDP.

```
shutdown lldp
no shutdown lldp
```

This command can be executed in Global Configuration Mode.

12.2 Set LLDP

This command Enables LLDP messages transmission.

```
set lldp {enable | disable}
```

This command can be executed in Global Configuration Mode.

12.3 Configure Global LLDP Parameters

These commands configure various LLDP parameters. The no version of the command restores default values.

```
lldp MessageFastTx <seconds(1-3600)>
lldp holdtime-multiplier <value(2-10)>
no lldp holdtime-multiplier
lldp notification-interval <seconds(5-3600)>
no lldp notification-interval
lldp reinitialization-delay <seconds(1-10)>
no lldp reinitialization-delay
lldp transmit-interval <seconds(5-32768)>
no lldp transmit-interval
lldp tx-delay <seconds(1-8192)>
no lldp tx-delay
lldp txCreditMax <value (1-10)>
lldp txFastInit <value (1-8)>
```

Parameter	Description
MessageFastTx	This command configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period. This value ranges from 1 to 3600 seconds.
holdtime-multiplier	This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. This value ranges from 2 to 10 seconds. Default value: 4
notification-interval	This command sets the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. This value ranges from 5 to 3600 seconds. Default: 5 seconds.
reinitialization-delay	This command sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission. This value ranges from 1 to 10 seconds. Default: 2 seconds.
transmit-interval	This command sets the transmission interval in which the server sends the LLDP frames to the LLDP module.This value ranges from 5 to 32768 seconds. Default: 30 seconds.
tx-delay	This command sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. This value ranges from 1 to 8192 seconds. Default: 2 seconds.
txCreditMax	This command configures the maximum number of consecutive LLDPDUs that can be transmitted any time. This value ranges from 1 to 10. Default: 5
txFastInit	This command configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode. This value ranges from 1 to 8. Default: 4.

This command can be executed in Global Configuration Mode.

12.4 Set LLDP Version

This command configures LLDP version to be used in the system.

```
set lldp version {v1 | v2}
```

Parameter	Description
v1	Enables LLDP 2005 version 1 on the port. This is the default value.
v2	Enables LLDP 2009 version 2 on the port.

This command can be executed in Global Configuration Mode.

12.5 LLDP Chassis-Id-Subtype

This command configures an ID for LLDP chassis subtype which is a unique address of any module.

```
lldp chassis-id-subtype { chassis-comp <string(255)> | if-alias | port-comp <string(255)> |
mac-addr | nw-addr | if-name | local <string(255)> }
```

Parameter	Description

chassis-comp	Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component.
if-alias	Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.
port-comp	Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.
mac-address	Represents a chassis identifier based on the value of a unicast source address, of a port on the chassis.
nw-addr	Represents a chassis identifier based on a network address,associated with a particular chassis. The encoded address is actually composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value.
if-name	Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.
local	Represents a chassis identifier based on a locally defined value.

This command can be executed in Global Configuration Mode.

12.6 Set LLDP-MED

This command enables or disables the LLDP-MED on the port.

```
set lldp-med {enable | disable}
```

This command can be executed in Interface Configuration Mode.

12.7 LLDP Interface-Related Parameters

12.7.1 LLDP Transmit | Receive

This command enables LLDP messages transmission or reception on the interface.

The no version of this command restores the default value

```
lldp {transmit | receive} [mac-address <mac_addr>]
```

Parameter	Description
transmit	Enables transmission of LLDPDU from one of the ports of the server to the LLDP module. It is enabled by default.
receive	Enables reception of LLDPDU from one of the ports of the server to the LLDP module. It is enabled by default.
mac-address	Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port

This command can be executed in Physical Interface Configuration Mode.

12.7.2 LLDP Destination MAC

This command configures destination mac-address to be used by the LLDP agent for transmission on this port.

The no form of the command resets the destination mac-address to LLDP multicast address .

```
lldp dest-mac <mac_addr>
```

```
no lldp dest-mac <mac_addr>
```

This command can be executed in Physical Interface Configuration Mode.

12.7.3 LLDP Med-App-Type

This command enables the properties of Network-policy TLV

The no form of the command disables the properties of Network-policy TLV.

The no version of this command restores the default value

```
lldp med-app-type {voice | voiceSignaling | guestVoice | guestVoiceSignaling |  softPhoneVoice
| videoconferencing | streamingVideo | videoSignaling} {vlan {untagged | vlan-id <integer(1-
4094)> priority <integer(0-7)>} dscp <integer (0-63)> | none}
no lldp med-app-type {voice | voiceSignaling | guestVoice | guestVoiceSignaling |
softPhoneVoice | videoconferencing | streamingVideo | videoSignaling}
```

Parameter	Description
voice	Sets the Network-policy TLV as Voice Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is voice.
voiceSignaling	Sets the Network-policy TLV as VoiceSignaling Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is VoiceSignaling.
guestVoice	Sets the Network-policy TLV as guestVoice Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is guestVoice.
guestVoiceSignaling	Sets the Network-policy TLV as guestVoiceSignaling Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is guestVoiceSignaling.
softPhoneVoice	Sets the Network-policy TLV as softPhoneVoice Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is softPhoneVoice.
videoconferencing	Sets the Network-policy TLV as videoconferencing Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is videoconferencing.
streamingVideo	Sets the Network-policy TLV as streamingVideo Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is streamingVideo.
videoSignaling	Sets the Network-policy TLV as videoSignaling Application for indicating that the media type defining a primary function of the application for the policy advertised on the local port is videoSignaling.
vlan	Configures VLAN to be enabled in the switch
untagged	Configures the ports that should be used for the VLAN to transmit egress packets as untagged packets.
vlan-id	VLAN ID is a unique value that represents the specific VLAN. This value ranges from 0 to 4094
priority	Configures the priority value for the VLAN. This value ranges from 0 to 7
dscp	Sets the DSCP value of the VLAN ID
none	Sets none of the port as static forward-all port for the VLAN

This command can be executed in Physical Interface Configuration Mode.

12.7.4 LLDP Med-Location

This command configures the location information advertised by the remote endpoint

The no form of the command disables the properties of Location information TLV.

```
lldp med-location { coordinate-location | civic-location } location-id <octet-string>
no lldp med-location { coordinate-location | civic-location | elin-location }
```

Parameter	Description
coordinate-location	Configures the co-ordinate location subtype.
civic-location	Configures the civic-location subtype
location-id	Configures the location identification. It is an octet string of value 16 for Coordinate and ranges from 6 to 256 for civic.

This command can be executed in Physical Interface Configuration Mode.

12.7.5 LLDP Med-Location ELIN-Location

This command configures the Emergency Location Information Number (ELIN) location subtype information advertised by the endpoint.

```
lldp med-location elin-location location-id <string(10-25)>
```

Parameter	Description
location-id	Configures the location identification.

This command can be executed in Physical Interface Configuration Mode.

12.7.6 LLDP Med-TLV-Select

This command enables the LLDP-MED TLV transmission on a given switch port.

The no form of this command disables the LLDP-MED TLV transmission on a given switch port.

```
lldp med-tlv-select { med-capability | network-policy | inventory-management | location-id |
ex-power-via-mdi } [ mac-address <mac_addr> ]
no lldp med-tlv-select { med-capability | network-policy | inventory-management | location-id |
ex-power-via-mdi } [ mac-address <mac_addr> ]
```

Parameter	Description
med-capability	Configures the Med Capability TLV transmission for the LLDP module.
network-policy	Configures the Network-policy TLV related transmission for the LLDP module.
inventory-management	Configures the Inventory-management TLV related transmission for the LLDP module.
location-id	Configures the Location identification TLV related transmission for the LLDP module.
ex-power-via-mdi	Configures the Extended power via MDI TLV related transmission for the LLDP module.
mac-address	Configures the basic TLV transmission to use the MAC address as destination MAC address by the LLDP agent on the specified switch port. Mac-address can be configured only if: • lldp version v2 is enabled

	• lldp dest-mac is configured

This command can be executed in Physical Interface Configuration Mode.

12.7.7 LLDP Notification

This command controls the transmission of LLDP notifications.

The no form of the command disables LLDP trap notification on an interface.

```
lldp notification ([remote-table-chg][mis-configuration]) [mac-address <mac_addr>]
no lldp notification [mac-address <mac_addr>]
```

Parameter	Description
remote-table-chg	Sends trap notification to NMS whenever remote table change occurs.
mis-configuration	Sends trap notification to NMS whenever misconfiguration is identified.
mac-address	Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port.

This command can be executed in Physical Interface Configuration Mode.

12.7.8 LLDP Port-Id-Subtype

This command configures an ID for LLDP port subtype

```
lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local
<string(255)> }
```

Parameter	Description
if-alias	Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.
port-comp	Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.
mac-addr	Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis.
if-name	Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.
local	Represents a chassis identifier based on a locally defined value.

This command can be executed in Physical Interface Configuration Mode.

12.7.9 LLDP TLV-Select

These commands enable the basic settings, configures dot1 or dor3 TLV apart basic settings, while transmitting the LLDP frames on a given port.

The no form of the command disables the basic TLV or dot1 or dot3 transmission on a given port.

```
lldp tlv-select basic-tlv { port-descr | sys-name | sys-descr | sys-capab | mgmt-addr {all |
ipv4 <ucast_addr> | ipv6 <ip6_addr>}} [mac-address <mac-address>]
lldp tlv-select dot1tlv { port-vlan-id | protocol-vlan-id {all |<vlan-id>} | vlan-name {all |
<vlan-id>} | vid-usage-digest | mgmt-vid | link-aggregation} [mac-address <mac_addr>]
lldp tlv-select dot3tlv { macphy-config | link-aggregation | max-framesize }
no lldp tlv-select basic-tlv { port-descr | sys-name | sys-descr | sys-capab |  mgmt-addr {all
| ipv4 <ucast_addr> | ipv6 <ip6_addr>}} [mac-address <mac_addr>]

no lldp tlv-select dot1tlv { port-vlan-id | protocol-vlan-id {all |<vlan-id>} | vlan-name {all
| <vlan-id>} | vid-usage-digest | mgmt-vid | link-aggregation }  [mac-address <mac_addr>]
```

```
no lldp tlv-select dot3TLV { macphy-config | link-aggregation | max-framesize }
```

Parameter	Description
port-descr	Enables the basic TLV transmission for the administratively assigned description for the port.
sys-name	Enables the basic TLV transmission for the administratively assigned system name.
sys-descr	Enables the basic TLV transmission for administratively assigned system description . The system description includes system's hardware name and type, and system's operating software and its version.
sys-capab	Enables the system capabilities of the basic TLV transmission.
mgmt-addr	Enables the basic TLV transmission to maintain the management addresses through which a management module can manage the system and allow the transmission on the current interface. • all - Enables the transmission of all the available management addresses on the current interface. If no management address is present/ configured in the system, switch mac-address will be taken for transmission. • ipv4 <ucast addr> - Enables the transmission of a particular ipv4 address on the current interface. • ipv6 <ip6 addr> - Enables the transmission of a particular ipv6 address on the current interface.
mac-address	Enables the basic TLV transmission to use the MAC address as destination MAC address by the LLDP agent on the specified port. Mac Address can be configured only if LLDP version is set as v2.
port-vlan-id	Specifies the VLAN ID of the port that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port.
protocol-vlan-id	Specifies the protocol ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This group ID is associated with the specific port. • all – Sets the protocol ID as all • <vlan-id> - Sets the protocol id as the mentioned vlan id. This value ranges from 1 to 4094.
vlan-name	Specifies the administratively assigned string, which is used to identify the VLAN. • all – Sets the protocol ID as all • <vlan-id> - Sets the protocol id as the mentioned vlan id. This value ranges from 1 to 4094.
vid-usage-digest	Performs dot1 TLV configuration while transmitting the LLDP frames to the VID usage digest TLV This parameter can be set only when LLDP version is set as v2.
mgmt-vid	Performs dot1 TLV configuration while transmitting the LLDP frames to the managemet VID TLV. This parameter can be set only when LLDP version is set as v2.
dot1 link-aggregation	Performs dot1 TLV configuration while transmitting the LLDP frames to the link-aggregation TLV.

	This parameter can be set only when LLDP version is set as v2.
macphy-config	Configures the physical MAC address of the TLV.
dot3 link-aggregation	Configures the link aggregation protocol statistics for each port on the device.
max-framesize	Configures the maximum frame size of the TLV

This command can be executed in Physical Interface Configuration Mode.

12.8 Show LLDP

This command displays various LLDP-related parameters.

```
show lldp
show lldp errors
show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]
show lldp local {[<interface-type> <interface-id> [mac-address <mac_addr>]] | [mgmt-addr]}
show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interfa
ce-type> <interface-id>][detail]
show lldp peers [chassis-id <string(255)> port-id <string(255)>] <interface-type> <interface-
id>[[mac-address <mac_addr>] [detail]]
show lldp statistics
show lldp traffic [<iftype> <ifnum> [mac-address <mac_addr>]]
show lldp peers
```

Parameter	Description
interface	This command displays the information about interfaces where LLDP is enabled.
interface-type	Displays the information about the specified type of interface.
interface-id	Displays the information about the specified interface identifier.
mac-address	Displays information about neighbors for the specidfied destination MAC address of the LLDP agent.
neighbors	This command displays information about neighbors on an interface or all interfaces.
detail	Displays the information obtained from all the received TLVs .
traffic	This command displays LLDP counters on all interfaces or on a specific interface. This includes the following: • Total Frames Out • Total Entries Aged • Total Frames In • Total Frames Received In Error • Total Frames Discarded • Total TLVS Unrecognized • Total TLVs Discarded
local	This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.
mgmt-addr	All the management addresses configured in the system and Tx enabled ports.
errors	This command displays the information about the errors such as memory allocation failures, queue overflows and table overflow.

statistics	This command displays the LLDP remote table statistics information.
peers	This command displays information about the peers on an interface or all interfaces.

This command can be executed in User or in Privileged Configuration Mode.

12.9 Clear LLDP Table

This command clears all the LLDP information about the neighbors.

```
clear lldp table
```

This command can be executed in Global Configuration Mode.

13 SYSLOG CONFIGURATION

Syslog is a protocol for capturing log information from devices in a network. The syslog protocol provides a transport allowing a node to send event notification messages across IP networks to event message collectors, also known as syslog servers.

One of the fundamental advantages of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a node without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

Syslog can be configured through CLI.

13.1 Logging

This command enables syslog server and configures the syslog related parameters. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server.

The no form of the command disables syslog server and resets the configured parameters. The existing syslog buffers will not be cleared and none of the configured options will be changed, when the syslog feature is disabled.

```
logging { buffered [<size (1-200)>] | console | facility {local0 | local1 | local2 | local3 |
local4 | local5 | local6 | local7|}| severity [{ <level (0-7)> | alerts | critical | debugging
| emergencies | errors | informational | notification | warnings }] | on }
no logging { buffered | console | facility | severity | on }
```

Parameter	Description
buffered	Limits Syslog messages displayed from an internal buffer. This size ranges between 1 and 200 entries.
console	Limits messages logged to the console.
facility	The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7.
severity	Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: • 0 | emergencies - System is unusable. • 1 | alerts - Immediate action needed. • 2 | critical - Critical conditions. • 3 | errors - Error conditions. • 4 | warnings - Warning conditions. • 5 | notification - Normal but significant conditions. • 6 | informational - Informational messages. • 7 | debugging – Debugging messages.
alerts	Immediate action needed.
critical	Critical conditions.
debugging	Debugging messages.
emergencies	System is unusable.
errors	Error conditions

informational	Information messages
notification	Normal but significant messages
warnings	Warning conditions.
on	Syslog enabled.

This command can be executed in Global Configuration Mode.

13.2 Logging-Server

This command configures a server table to log an entry in it.

The no form of command deletes an entry from the server table.

```
logging-server <short(0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> | <dns_host_name>} [port
<integer(1-65535)>] [{udp | tcp}]
```

Parameter	Description
short	Sets the priority for the syslog messages which decides the order in which it is to be forwarded to the desired server. 0-lowest priority, 191-highest priority. This value ranges from 0 to 191.
ipv4	Sets the server address type as internet protocol version 4 and configures the IPv4 address of the server.
ipv6	Sets the server address type as internet protocol version 6 and configures the IPv6 address of the server.
dns_host_name	Configures the DNS host name for a server to log an entry. This value is a string of maximum size 255.
port	Sets the port number through which the server sends the syslog message. This value ranges from 1 to 65535. Default port is 514.
udp	Sets the forward transport type as udp. This is the default transport.
tcp	Sets the forward transport type as tcp.

This command can be executed in Global Configuration Mode.

13.3 Show Logging-Server

This command displays the information about the syslog logging server table.

```
show logging-server
```

This command can be executed in User or in Privileged Mode.

13.4 Show Logging

This command displays all the logging status and configuration information.

```
show logging
```

This command can be executed in User or in Privileged Mode.

14 SNMP CONFIGURATION

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol in TCP/IP-based networks. SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) and VACM (View based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees. Also, SNMPv3 specifies a generic management framework, which is expandable for adding new Management Engines, Security Models, Access Control Models and so on. With SNMPv3, the SNMP communication is completely safe and secure.

GigaFlex SNMP Agent supports all three versions of SNMP (SNMPv1, SNMPv2c and SNMPv3) while conforming to the latest specifications.

14.1 Supported MIBs

The following MIBs are supported:

- IEEE8021-PAE-MIB stdpnac.mib
- LLDP-MIB stdlldp.mib
- LLDP-EXT-DOT3-MIB stdot3lldp.mib
- LLDP-EXT-MED-MIB stdlldpmedx.mib
- LLDP-EXT-DOT1-MIB stdot1lldp.mib
- LLDP-EXT-DOT3-V2-MIB stdot3lldpv2.mib
- LLDP-EXT-DOT1-V2-MIB stdot1lldpv2.mib
- IEEE8023-LAG-MIB stdla.mib
- SNMPv2-MIB stdsnmp.mib
- IF-MIB ifmib.mib
- IP-MIB stdipvx.mib
- TCP-MIB stdtcp.mib
- UDP-MIB stdudpipvx.mib
- EtherLike-MIB stdether.mib
- OSPF-MIB stdospf.mib
- RMON2-MIB stdrmon2.mib
- BRIDGE-MIB stdbridge.mib
- RSTP-MIB stdrst.mib
- STDRIP2-MIB stdrip.mib
- MAU-MIB stdmau.mib
- DNS-RESOLVER-MIB stddns.mib
- ENTITY-MIB stdent.mib
- IPV6-MIB stdipv6.mib
- RADIUS-AUTH-CLIENT-MIB radauth.mib
- RADIUS-ACC-CLIENT-MIB radacc.mib
- VRRP-MIB stdvrrp.mib
- IPMROUTE-STD-MIB stdmri.mib
- DIFFSERV-MIB stdqos.mib
- VRRPV3-MIB stdvrrp3.mib
- PIM-MIB stdpim.mib
- OSPFV3-MIB ospf3.mib
- NATEKS-G826-MIB gg826.mib
- NATEKS-DSL-MIB gshdsl.mib
- NATEKS-DDM-MIB gddm.mib
- NATEKS-IO-MIB gio.mib

- NATEKS-RS232-MIB grs232.mib
- GEMINI-IP-MIB fsip.mib
- GEMINI-OSPF-MIB fsospf.mib
- GEMINI-OSPF-TEST-MIB fsostest.mib
- GeminiNat-MIB fsnat.mib
- FIREWALL-MIB fsfwl.mib
- GEMINI-TCP-MIB fstcp.mib
- GEMINI-PIM-MIB fspim.mib
- GEMINI-DHCP-RLY-MIB fsdhcpRelay.mib
- GEMINI-RADIUS-MIB fsradius.mib
- GEMINI-CFA-MIB fscfa.mib
- GEMINI-IPV6-MIB fsipv6.mib
- GEMINI-IGMP-MIB fsigmp.mib
- GEMINI-RMON-MIB fsrmon.mib
- GEMINI-LA-MIB fsla.mib
- GEMINI-PNAC-MIB fspnac.mib
- GEMINI-IPV6-MLD-MIB fsmld.mib
- GEMINI-RIP2-MIB fsrip.mib
- GEMINI-ISS-MIB fsiss.mib
- GEMINI-ISS-EXT-MIB fsissext.mib
- GEMINI-DHCP-SERVER-MIB fsdhcps.mib
- GEMINI-SYSLOG-MIB fssyslg.mib
- GEMINI-OSPFV3-MIB fsos3.mib
- GEMINI-RTM6-MIB fsrtm6.mib
- VCM-MIB fsvcm.mib
- GEMINI-SSL-MIB fsssl.mib
- GEMINI-SSH-MIB fssshmib.mib
- GEMINI-POE-MIB fspoe.mib
- GEMINI-SNOOP-MIB fssnp.mib
- GEMINI-RTM-MIB fsrtm.mib
- GEMINI-ARP-MIB fsarp.mib
- GEMINI-PIMCMN-MIB fspimcmn.mib
- GEMINI-SNMP3-MIB fssnmp3.mib
- GEMINI-PIMCMN2-MIB fspimstd.mib
- GEMINI-MIStdBRIDGE-MIB fsmsbrg.mib
- GEMINI-MIStdRSTP-MIB fsmsrst.mib
- GEMINIP-BRIDGE-MIB fsbridge.mib
- GEMINIQ-BRIDGE-MIB fsmsvlan.mib
- GeminiMIMst-MIB fsmpmst.mib
- GEMINI-MIRSTP-MIB fsmprst.mib
- GeminiMIVlan-MIB fsmpvlan.mib
- GEMINI-OSPFMI-MIB fsmiospf.mib
- GEMINI-MISTDOSPF-MIB fsmistdospf.mib
- GEMINI-OSPFMI-TRAP-MIB fsstdmiostrp.mib
- FSSNTP-MIB fssntp.mib
- GEMINI-MIRIP2-MIB fsmirip.mib
- GEMINI-MISTDRIP2-MIB fsmistdrip.mib
- GEMINI-VRRP-MIB fsvrrp.mib

SNMP can be configured either through CLI or in WEB on General Settings → Services Page

14.2 SNMPAGENT

This command enables or disables SNMP agent. The SNMP Agent is enabled by default.

```
enable snmpagent
disable snmpagent
```

This command can be executed in Global Configuration Mode.

14.3 SNMP Community

This command configures SNMP Community.

The no form of this command removes the SNMP community details.

```
snmp community <string(32)> version {v1 | v2c} view-type [read] [write] [notify]
no snmp community <string(32)> version {v1 | v2c}
```

Parameter	Description
community	Creates a community name which stores the community string.
version	Set SNMP version to v1 or v2c
read	Gives read permissions to this community
write	Gives write permissions to this community

This command can be executed in Global Configuration Mode.

14.4 SNMP TARGETADDR

This command configures the SNMP target address. This is the destination address used for delievery of SNMP messages.

The no form of the command removes the configured SNMP target address.

```
snmp targetaddr {<ucast_addr> | <ip6_addr> | <dns_host_name>} username <string(32)>
no snmp targetaddr <TargetAddressName>
```

Parameter	Description
ucast_address	Configures a unicast target address to which the generated SNMP notifications are sent.
IP6Address	Configures a IP6 target address to which the generated SNMP notifications are sent.
dns_host_name	Configures the DNS host name to which the generated SNMP notifications are sent. This value is a sting of maximum size 255.
username	SNMP v1 | v2c community or SNMP v3 Username that will be used in the notifications.

This command can be executed in Global Configuration Mode.

14.5 SNMP User

This command configures the SNMP v3 user details.

The no form of the command removes the SNMP user details.

```
snmp user <UserName> [auth {md5 | sha} <passwd> [priv {{DES | AES_CFB128} <passwd>}]] view-type
[read] [write] [notify]
no snmp user <UserName>
```

Parameter	Description
UserName	Configures an User name for SNMP v3.
auth	Sets an authentication Algorithm . Options are: • md5 - Sets the Message Digest 5 based authentication. • sha - Sets the Security Hash Algorithm based authentication.
passwd	Sets the authentication password that will be used for the configured authentication algorithm.
priv	Sets the encryption and also the password to be used for the encryption key. Options are: • DES – Configures the data encryption standard algorithm related configuration. • AES_CFB128 – Configures Advanced Encryption Standard (AES) algorithm for encryption. • <Passwd> - Sets the authentication password that will be used for the configured authentication algorithm. • None - Sets encryption configuration as none.
view-type	Configures the rights for the user: • Read – the User has rights to read SNMP information. • Write – the User has rights to write SNMP information. • Notify – the User had riggts to send SNMP notifications.

This command can be executed in Global Configuration Mode.

14.6 SNMP-Server Enable Traps

This command enables generation of various traps from the SNMP agent (for all snmpv1, snmpv2 and snmpv3).

The no form of the command disables generation of traps.

```
snmp-server enable traps snmp authentication
no snmp-server enable traps snmp authentication
snmp-server enable traps coldstart
no snmp-server enable traps coldstart
```

Parameter	Description
Authentication	Configures authentication Trap.
coldstart	Configures coldstart Trap.

This command can be executed in Global Configuration Mode.

14.7 Show SNMP <Parameters>

This command displays various SNMP-related parameters.

```
show snmp
show snmp community
show snmp group
```

```
show snmp engineID
show snmp targetaddr
show snmp targetparam
show snmp user
show snmp-server traps
```

Parameter	Description
community	Shows SNMP Communty.
group	Shows SNMP group information.
engineID	Show SNMP EngineID
targetaddr	Shows SNMP Target Address.
targetparam	Show SNMP Target Parameters.
user	Show SNMP Users
snmp-server traps	This command displays the set of traps that are currently enabled.

This command can be executed in User or in Privileged Mode.

15 RMON CONFIGURATION

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

RMON can be configured trough CLI.

15.1 Set RMON

This command is used to enable or disable the RMON feature.

```
set rmon {enable | disable}
```

Parameter	Description
enable	Enables the RMON feature in the system. On enabling, the RMON starts network monitoring and provides network fault diagnosis.
disable	Disables the RMON feature in the system. On disabling, the RMON's network monitoring is shutted down.

This command can be executed in Global Configuration Mode.

15.2 RMON Collection Stats

This command enables RMON statistic collection on the interface or on VLAN.

The no form of the command disables RMON statistic collection on the interface or on VLAN.

```
rmon collection stats <index (1-65535)> [owner <ownername (127)>]
no rmon collection stats <index (1-65535)>
```

Parameter	Description
index	Identifies an entryin the statistics table.. This value ranges from 1 to 65535.
owner	Configures the the name of the owner of the RMON group of statistics.

This command can be executed in Interface / VLAN Configuration Mode.

15.3 RMON Collection History

This command enables history collection of interface/ VLAN statistics in the buckets for the specified time interval.

The no form of the command disables the history collection on the interface/VLAN.

```
rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval
<seconds (1-3600)>] [owner <ownername (127)>]
no rmon collection history <index (1-65535)>
```

Parameter	Description
index	Identifies an entry in the history control table. Each such entry defines a set of samples at a particular interval for an interface on the device. This value ranges from 1 to 65535.
buckets	Configures the number of buckets desired for the RMON collection history group of statistics. This is the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table

	associated with this History Control EntryThe polling cycle is the bucket interval where the interface statistics details are stored. This value ranges from 1 to 65535.
interval	Configures the time interval over which the data is sampled for each bucket. This value ranges from 1 to 3600.
owner	Configures the name of the owner of the RMON group of statistics:

This command can be executed in Interface / VLAN Configuration Mode.

15.4 RMON Event

This command adds an event to the RMON event table. The added event is associated with an RMON event number.

The no form of the command deletes an event from the RMON event table.

```
rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername
(127)>] [trap <community (127)>]
no rmon event <number (1-65535)>
```

Parameter	Description
number	Sets the number of events to be added in the event table. This value ranges from 1 to 65535.
description	Provides a description for the event. This value is a string with a maximum length of 127.
log	Creates an entry in the log table for each event.
owner	Displays the entity that are configured this entry. This value is a string with a maximum value of 127.
trap	Generates a trap, The SNMP community string is to be passed for the specified trap. This value is a string with a maximum value of 127.

This command can be executed in Global Configuration Mode.

15.5 RMON Alarm

This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured.

The no form of the command deletes the alarm configured on the MIB object.

```
rmon alarm <alarm-number> <mib-object-id (255)> <sample-interval-time (1-65535)> {absolute |
delta} rising-threshold <value (0-2147483647)> [rising-event-number (1-65535)] falling-
threshold <value (0-2147483647)> [falling-event-number (1-65535)] [owner <ownername (127)>]
no rmon alarm <number (1-65535)>
```

Parameter	Description
alarm-number	Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds. This value ranges from 1 to 65535.
mib-object-id	Identifies the mib object.

sample-interval-time	Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. This value ranges from 1 to 65535 seconds.
absolute	Compares the value of the selected variable with the thresholds at the end of the sampling interval.
delta	Subtracts the value of the selected variable at the last sample from the current value, and the difference is compared with the thresholds at the end of the sampling interval.
rising-threshold	Configures the rising threshold value. If the startup alarm is set as Rising alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated. This value ranges from 0 to 2147483647.
rising-event-number	Raises the index of the event, when the Rising threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges from 1 to 65535.
falling-threshold	Configures the falling threshold value. If the startup alarm is set as Falling alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is lesser than or equal to the configured Falling threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated. This value ranges from 0 to 2147483647.
falling-event-number	Raises the index of the event when the Falling threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges from 1 to 65535.
owner	Sets the entity that are configured this entry.

This command can be executed in Global Configuration Mode.

15.6 Show RMON

This command displays the RMON statistics, alarms, events, and history configured on the interface.

```
show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]
```

Parameter	Description
statistics	Displays a collection of statistics for a particular Ethernet Interface. The probe for each monitored interface on this device measures the statistics.
alarms	Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed.
events	Generates events whenever an associated condition takes place in the device. The Conditions may be alarms. Alarms are generated when a sampled statistical variable value exceeds the defined threshold value. Alarm module calls events module.
history	Displays the history of the configured RMON.
overview	Displays only the overview of RMON history entries.

This command can be executed in User or in Privileged Mode.

16 MULTICAST CONFIGURATION

16.1 IGMP Snooping

The Internet Group Multicast Protocol, (IGMP) is the protocol, a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGMP Snooping (IGS) is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. In IGMP Snooping, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, it can learn the multicast sessions to which other computers on the local network are listening. The multicast packet transfer happens only between the source and the destination computers. Broadcasting of packets is avoided. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

IGMP Snooping can be configured either through CLI or in WEB on Switching → IGMP Snooping Page.

16.1.1 IP IGMP Snooping

This command enables IGMP snooping in the switch or in a specific VLAN. When snooping is enabled in a switch or interface, it learns the hosts intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it forwards the packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces.

The no form of the command disables IGMP snooping in the switch or in a specific VLAN. When IGMP snooping is disabled globally, it is disabled in all the existing VLAN interfaces.

```
ip igmp snooping [vlan <vlan-id>]
no ip igmp snooping [vlan <vlan-id>]
```

Parameter	Description
vlan-id	VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.

This command can be executed in Global Configuration Mode.

16.1.2 IP IGMP Snooping Enhanced-Mode

This command configures snooping system enhanced mode in the switch. It is a mode of operation provided to enhance the operation of IGMP snooping module to duplicate Multicast traffic by learning Multicast group entries based on the Port and Inner VLAN. This mode of operation is applied when the downstream devices are less intelligent or not capable of duplicating Multicast traffic.

```
ip igmp snooping enhanced-mode { enable | disable }
```

Parameter	Description
enable	Enables snooping system enhanced mode in the switch.
disable	Disables snooping system enhanced mode in the switch

This command can be executed in Global Configuration Mode.

16.1.3 IP IGMP Snooping Filter

This command configures the IGMP snooping filter. The IGS filtering feature restricts channel registration from being added to the database. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream. When disabled, all the filter related configurations remain but the incoming reports will not be subject to filtering. IGMP Snooping module programs the hardware to remove the configured rate limit. It flushes all the registrations learnt through a port if a threshold limit is configured for this interface.

The no form of the command disables the IGMP snooping filter. It's a default value.

```
ip igmp snooping filter
no ip igmp snooping filter
```

This command can be executed in Global Configuration Mode.

16.1.4 IP IGMP Snooping Sparse-Mode

This command configures snooping system sparse mode in the switch. In the sparse mode, the IGMP Snooping module drops the unknown multicast traffic when there is no listener for the multicast data. In the non-sparse-mode, the IGMP Snooping module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of VLAN.

```
ip igmp snooping enhanced-mode { enable | disable }
```

Parameter	Description
enable	Enables snooping system sparse mode in the switch. Drops unknown multicast packets.
disable	Disables snooping system sparse mode in the switch. Floods unknown multicast packets. This is dafault setting.

This command can be executed in Global Configuration Mode.

16.1.5 IP IGMP Snooping Multicast-VLAN

This command configures the multicast VLAN feature on a port. Multicast VLAN feature is used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through VLANs.

```
ip igmp snooping multicast-vlan {enable | disable}
```

Parameter	Description
enable	Enables the multicast Vlan feature. Router sends a single copy of the data for the particular MVLAN, instead of forwarding a separate copy of the multicast data to each VLAN. This saves the network bandwidth.
disable	Disables the multicast Vlan feature. A separate copy of the multicast data has to be forwarded from the router in the absence of M-VLAN. This is default setup.

This command can be executed in Global Configuration Mode.

16.1.6 IP IGMP Snooping Query-Forward

This command configures the IGMP queries to be forwarded to all VLAN member ports or only to non-router ports. This configuration directs the queries to the selected ports to avoid flooding of the network. The queries are forwarded to multicast groups.

```
ip igmp snooping query-forward {all-ports | non-router-ports}
```

Parameter	Description
all-ports	Configures the IGMP query forward administrative control status as all VLAN member ports. This is done to find out if there are any interested listeners in the network.
non-router-ports	Configures the IGMP query forward administrative control status as non-router ports only. This is done to reduce the traffic in the network. This is the default value.

This command can be executed in Global Configuration Mode.

16.1.7 IP IGMP Snooping Report-Forward

This command configures the IGMP reports to be forwarded to all ports, router ports of a VLAN or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network.

The no form of the command sets IGMP report-forwarding status to default value.

```
ip igmp snooping report-forward {all-ports | router-ports | non-edge-ports }
no ip igmp snooping report-forward
```

Parameter	Description
all-ports	Configures the IGMP reports to be forwarded to all the ports of a VLAN.
router-ports	Configures the IGMP reports to be forwarded only to router ports of a VLAN. This is the default value.
non-edge-ports	Configures the IGMP reports to be forwarded only to STP non edge ports.

This command can be executed in Global Configuration Mode.

16.1.8 IP IGMP Snooping Send-Query

This command configures the IGMP general query transmission feature upon the topology change in the switch.

```
ip igmp snooping send-query { enable | disable }
```

Parameter	Description
enable	Enables the snooping query transmission status which generates IGMP query messages.
disable	Disables the snooping query transmission status which stops the switch from generating IGMP query messages. This is default value.

This command can be executed in Global Configuration Mode.

16.1.9 IP IGMP Snooping VLAN MROUTER

This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN.

Any IGMP message received on a switch is forwarded only on the router-ports and not on host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.

The no form of the command deletes the statically configured router ports for a VLAN.

```
ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>
```

```
no ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>
```

Parameter	Description
vlan-id	Configures the VLAN for which the list of multicast router ports should be configured statically. This is a unique value that represents the specific L3 VLAN created. An L3 VLAN interface is a VLAN that is mapped to an IP interface and assigned an IP address. This value ranges from 1 to 4094.
ifXtype	Interface type: gigabitethernet or gi.
0/a-b, 0/c, ...	List of ports.

This command can be executed in Global Configuration Mode.

16.1.10 IP IGMP Snooping VLAN Immediate-Leave

This command enables fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094.

The no form of the command disables fast leave processing for a specific VLAN. It is the default behaviour.

```
ip igmp snooping vlan <vlanid(1-4094)> immediate-leave
no ip igmp snooping vlan <vlanid(1-4094)> immediate-leave
```

Parameter	Description
vlan-id	Configures the VLAN for which the list of multicast router ports should be configured statically. This is a unique value that represents the specific L3 VLAN created. An L3 VLAN interface is a VLAN that is mapped to an IP interface and assigned an IP address. This value ranges from 1 to 4094.

This command can be executed in Global Configuration Mode.

16.1.11 IP IGMP Snooping Counters and Timers

The following commands allow configuration of IGMP Snooping Counters and Timers.

The no version of these commands restores default settings.

```
ip igmp snooping group-query-interval <(2 - 5) seconds>
no ip igmp snooping group-query-interval
ip igmp snooping mrouter-time-out <(60 - 600) seconds>
no ip igmp snooping mrouter-time-out
ip igmp snooping port-purge-interval <(130 - 1225) seconds>
no ip igmp snooping port-purge-interval
ip igmp snooping report-suppression-interval <(1 - 25) seconds>
no ip igmp snooping report-suppression-interval
ip igmp snooping retry-count <1 - 5>
no ip igmp snooping retry-count
```

Parameter	Description
group-query-interval	This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. This value ranges from 2 to 5. The no form of the commands sets the group specific query interval time to default value: 2 seconds

mrouter-time-out	This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learnt router port. The router sends control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds. The no form of the command sets the IGMP snooping router port purge time-out to default value: 125 seconds.
port-purge-interval	This command configures the IGMP snooping port purge time interval. When the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds. The no form of the command sets the IGMP snooping port purge time to default value.
report-suppression-interval	This command sets the IGMP snooping report-suppression time interval. The switch forwards IGMPv2 report message to the multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval the switch does not forward another IGMPv2 report message addressed to the same multicast group to the router ports. The no form of the command sets the IGMP snooping report-suppression interval time to the default value.
retry-count	This command sets the maximum number of group specific queries sent by the switch to check if there are any interested v2 receivers for the group when it receives a leave message in the proxy/ proxy-reporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number. This value ranges from 1 to 5. The no form of the command sets the number of group specific queries sent by the switch on reception of leave message to default value: 2

This command can be executed in Global Configuration Mode.

16.1.12 Show IP IGMP Snooping

This command displays various IGMP-Snooping related parameters.

```
show ip igmp snooping [Vlan <vlan-id>]
show ip igmp snooping blocked-router [Vlan <vlan-id>]
show ip igmp snooping forwarding-database [Vlan <vlan-id>] [{static | dynamic}]
show ip igmp snooping globals
show ip igmp snooping groups [Vlan <vlan-id> [Group <Address>]] [{static | dynamic}]
show ip igmp snooping mrouter [Vlan <vlan-id>] [detail]
show ip igmp snooping multicast-receivers [Vlan <vlan-id> [Group <Address>]]
show ip igmp snooping multicast-vlan
show ip igmp snooping port-cfg [{interface <interface-type> <interface-id> [InnerVlanId vlan-
id(1-4094)]}]
show ip igmp snooping statistics [Vlan <vlan-id>]
```

Parameter	Description
show ip igmp snooping	This command displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the contexts (if no switch is specified).
blocked-router	This command displays the blocked router ports for all VLANs or a specific VLAN.
forwarding-database	This command displays multicast forwarding entries for all VLANs or a specific VLAN. It also displays the information for static / dynamic or both types of multicast entries. • Static - Display the static multicast forwarding entries. • Dynamic - Display the dynamic multicast forwarding entries. If not specified, both static and dynamic entries are displayed.
globals	This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified).
groups	This command displays IGMP group information for all VLANs or a specific VLAN. It also displays the information for static / dynamic or both types of multicast entries.
mrouter	This command displays the router ports for all VLANs or a specific VLAN. The interface details and the corresponding port number along with its type (static/dynamic are displayed.
multicast-receivers	This command displays IGMP multicast host information for all VLANs or a specific VLAN.
multicast-vlan	This command displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs.
port-cfg	This command displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId.
Statistics	This command displays IGMP snooping statistics for all VLANs or a specific VLAN.

This command can be executed in Global Configuration Mode.

16.2 IGMP

GigaFlex firmware implements the Internet Group Management Protocol Version 3. It implements the IGMP router functionalities required by the Multicast Routing Protocol.

The IGMP realisation confirms with RFC 3376 for IGMP v3 router functionality. The IGMP supports the MIB defined in draft-ietf-magma-rfc2933-update-00.txt.

The deployment of the IGMP router can be done within a routing domain that uses any Multicast Routing Protocol. The IGMP informs MRPs about group membership messages and leave messages.

The IGMP can be configured either through Command Line or in WEB on Multicast Page.

16.2.1 Set IP IGMP

This command enables or disables IGMP globally or on an interface.

```
set ip igmp {enable|disable}
```

Parameter	Description
enable	Enables IGMP feature globally or on a particular interface.
disable	Disables IGMP feature globally or on a particular interface. This removes all dynamic multicast entries, stop all the timers for route entries and disables IGMP on all the IGMP enabled interfaces. IGMP is disabled by default.

This command can be executed in Global or in Interface Configuration Mode.

16.2.2 IP IGMP Version

This command configures the IGMP version on the interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.

The no form of the command sets the default IGMP version on the interface.

```
ip igmp version { 1 | 2 | 3}
no ip igmp version
```

Parameter	Description
value	Configures the IGMP version according to the value. Default vesion is 2.

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.2.3 IP IGMP Static-Group

This command adds the static group membership on the interface.

The no form of the command deletes the static group membership on the interface.

```
ip igmp static-group <Group Address> [source <Source Address>]
no ip igmp static-group <Group Address> [source <Source Address>]
```

Parameter	Description
Group Address	Configures the group IP address as a static group member on the interface.
source	Configures the source IP address of a system where multicast data packets originate.

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.2.4 IP IGMP Explicit-Tracking

This command enables explicit channel tracking on IGMPv3 interface. Channel tracking is the ability of a system to keep track of each individual host that is joined to a particular multicast group or channel.

The no form of the command disables explicit channel tracking on IGMPv3 interface.

```
ip igmp explicit-tracking
no ip igmp explicit-tracking
```

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.2.5 IP IGMP Immediate-Leave

This command enables immediate leave processing on the interface by intimating to the Multicast Routing Protocol on the last member leaving the group. This must be enabled only on those interfaces where there is single host. This feature can also be enabled on those interfaces having more than one hosts only if all are v3 hosts in V3 Mode.

The no form of the command disables immediate-leave processing on the interface.

```
ip igmp immediate-leave
no ip igmp immediate-leave
```

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.2.6 IP IGMP Configuration Parameters and Timers

The following commands configure various IGMP parameters and timers. The no form of a command restores default values.

```
ip igmp join ratelimit <value(100-1000)>
no ip igmp join ratelimit
ip igmp last-member-query-interval <value(1-255) tenths of seconds>
no ip igmp last-member-query-interval
ip igmp limit <value(1-4096)> [except <Group-List id>]
no ip igmp limit
ip igmp query-interval <value (1-31744) seconds>
no ip igmp query-interval
ip igmp query-max-response-time <value (1-255) tenths of seconds>
no ip igmp query-max-response-time
ip igmp robustness <value(2-7)>
no ip igmp robustness
```

Parameter	Description
join ratelimit	This command configures the Join Rate limit for a downstream interface in number of IGMP packets per second. This value ranges from 100 to 1000. The no form of the command resets the Join Rate limit to its default value that is 0.
last-member-query-interval	This command configures the IGMP last member query interval for the interface. The last member query interval is the maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. This value is tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This value ranges from 1 to 255 tenths of seconds. The no form of the command sets the last member query interval to its default value that is 10.
limit	This command configures global group limit for IGMP.This value is the total number of multicast groups allowed globally and ranges from 1 to 255. The no form of the command deletes the global group limit for IGMP. This takes the default value 0.
query-interval	This command configures the frequency at which IGMP host-query packets are transmitted on the interface. This value ranges from 1 to 31744 seconds. The no form of the command resets the IGMP query-interval to its default value 125 seconds.
query-max-response-time	This command configures the maximum IGMP query response value for the interface. This value ranges from 1 to 255 tenths of seconds.

	The no form of the command resets the max query response to its default value 100 seconds.
robustness	This command configures the IGMP robustness value for the interface. This value ranges from 2 to 7. The robustness variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness value may be increased. The no form of the command resets the robustness value to its default value 2.

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.2.7 Show IP IGMP

This command displays various IGMP-related parameters.

```
show ip igmp global-config
show ip igmp group-list
show ip igmp groups
show ip igmp interface [{ Vlan <vlan-id> | <interface-type> <interface-id> | <IP-interface-
type> <IP-interface-number>}]
show ip igmp membership [[<mcast_addr>] {[tracked] | [all]}]
show ip igmp sources
show ip igmp statistics [{ Vlan <vlan-id> | <interface-type> <interface-id> | <IP-interface-
type> <IP-interface-number>}]
```

Parameter	Description
global-config	This command displays the global configuration of IGMP.
group-list	This command displays all the global group -list of IGMP.
groups	This command displays the IGMP group information.
interface	This command displays the interface configuration of IGMP.
membership	This command displays the membership information for groups or channels. • <mcast addr> - Displays membership information for multicast groups. • all - Displays the membership Displays the membership information all m ulticast groups. • tracked - Displays the membership information information for the multicast groups for which channel tracking is enabled.
sources	This command displays the IGMP source information.
statistics	This command displays the IGMP statistics information.

This command can be executed in User or in Privileged Mode.

16.3 PIM

PIM (Protocol Independent Multicast) is a multicast routing architecture that allows IP multicast routing in existing IP network. Multicast IP Routing protocols are used to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients. A multicast group identifies a set of recipients that are interested in a particular data stream and is represented by a multicast IP address. Data sent to this IP address is forwarded to all members of the multicast group.

PIM is independent from unicast routing protocol and can be operated in two modes: dense and sparse. It is designed to provide scalable inter-domain multicast routing across the Internet. PIM provides multicast routing and forwarding capability to the unit. It maintains the integrity of the hardware-based multicast forwarding table. It is independent from the underlying unicast routing protocol but uses the information from it.

The PIM can be configured either through CLI or in WEB in Routing → Multicast Page.

16.3.1 Set IP PIM

```
set ip pim { enable | disable }
```

Parameter	Description
enable	Enables PIM feature in the unit.
disable	Disables PIM feature in the unit.

This command can be executed in Global Configuration Mode.

16.3.2 IP PIM Version

This command configures version number of the PIM protocol in the switch.

```
ip igmp version { 1 | 2 | 3}
no ip igmp version
```

Parameter	Description
value	Configures the PIM version according to the value. Default vesion is 2.

This command can be executed in Global Configuration Mode.

16.3.3 IP PIM BIDIR-Enable

This command enables the Bidirectional PIM feature.

Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potentially receivers also.

The no form of the command disables the Bidirectional PIM feature. It's disabled by default.

```
ip pim bidir-enable
no ip pim bidir-enable
```

This command can be executed in Global Configuration Mode.

16.3.4 IP PIM BIDIR-Offer

This command configured PIM Bidirectional Offer parameters. The no version of this command restores the default value.

```
ip pim bidir-offer-interval <offer-interval> msecs
no ip pim bidir-offer-interval
ip pim bidir-offer-limit <offer-limit-integer>
no ip pim bidir-offer-limit
```

Parameter	Description
interval	This command configures the Bidir-PIM offer interval in milliseconds. It is the time interval between the Distance Forwarder (DF) election Offer messages to be sent. This value ranges from 1 to 20000000.milliseconds

	The no form of the command resets the PIM Bidir-PIM offer interval to the default value 100 miliseconds.
limit	This command configures the Bidir-PIM offer limit, the number of unanswered offers before the router changes as the designated forwarder (DF). This value ranges from 3 to 100. The no command sets the Bidir- PIM offer-limit to the default value: 3.

This command can be executed in Global Configuration Mode.

16.3.5 IP PIM State-Refresh Disable

This command disables the SRM processing and forwarding, that is, the router drops the State Refresh Messages, if received and also the router will not advertise the SR Capability in Hello messages.

The no form of the command enables the SRM processing and forwarding. On enabling, this router advertises itself as SR Capable in Hello Messages.

```
ip pim state-refresh disable
no ip pim state-refresh disable
```

This command can be executed in Global Configuration Mode.

16.3.6 IP PIM Component

This command configures the PIM component in the router and enters into pim component mode. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode.

The no form of the command destroys the PIM component. This value ranges from 2 to 255.

The PIM Component 1 cannot be deleted as it is the default component.

```
ip pim component <ComponentId (1-255)> [Scope-zone-name(64)]
no ip pim component <ComponentId (2-255)>
```

Parameter	Description
ComponentId	Configures the PIM component in the router and enters into pim component mode. This value ranges from 1 to 255
Scope-zone-name	Configures the scope-zone-name. The maximum length of the string is 64. To configure the scope-zone name , scope-zone should be created in the interface. Scope is a 4-bit value that describes the scope of an IPV6 address. A unicast address can possibly have 2 scopes (Linklocal and Global) only and a multicast address can have a maximum of 11 scopes. The scope zone name should be the same as that of the zone created in the ipv6 scope zone command. If ipv6 scope-zone is created as scopeA 1, then the scope zone name should be scopeA1. (Without space).

This command can be executed in Global Configuration Mode.

16.3.7 IP PIM BSR-Border

This command sets a PIM domain BSR (Bootstrap router) message border for an interface which stops the BSR message forwarding over the specified interface.

The no form of the command resets the PIM domain BSR message border

```
ip pim bsr-border
```

```
no ip pim bsr-border
```

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.3.8 IP PIM BSR-Candidate

This command configures the preference value for the local interface as a candidate Bootstrap Router (BSR). This preference value ranges between 0 and 255.

A BSR is a dynamically elected router within a PIM domain. The router with highest priority is considered as the BSR. If the priority values are same, then the router with largest IP address is considered as the BSR.

The no form of the command resets the default preference value for the local interface as a candidate bootstrap router.

```
ip pim bsr-candidate <value (0-255)>
no ip pim bsr-candidate
```

Parameter	Description
value	Local Interface weifgt. Default 0.

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.3.9 IP PIM COMPONENTID

This command adds the interface to the PIM component. This value ranges from 1 to 255. This command adds the current VLAN into the specified PIM component.

The no form of the command removes the interface from the PIM component

```
ip pim componentId  <value(1-255)>
no ip pim componentId
```

Parameter	Description
value	PIM Component Value. Default 1.

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.3.10 IP PIM DR-Priority

This command configures the designated router priority value configured for the router interface. This value ranges from 1 to 4294967295.

The no form of the command sets the default designated router priority value for the router interface.

The DR sets up multicast route entries and sends corresponding Join/Prune and Register messages on behalf of directly-connected receivers and sources, respectively.

```
ip pim dr-priority <priority>
no ip pim dr-priority
```

Parameter	Description
priority	Interface priority. Default 1.

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.3.11 IP PIM External Border

This command sets an external non-PIM domain BSR message border for an interface which stops the BSR message forwarding over the specified interface.

The no form of the command resets the external non-PIM domain BSR message border.

```
ip pim external border
no ip pim external border
```

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.3.12 PIM Protocol Timers

This command configures various PIM protocol-related timers. The no version of this command restores default value.

```
ip pim lan-delay <value(0-65535) milliseconds>
no ip pim lan-delay
ip pim message-interval <Interval(10-600) seconds>
no ip pim message-interval
ip pim override-interval <interval(5-65535) milliseconds>
no ip pim override-interval
ip pim query-interval <Interval(1-18725) seconds>
no ip pim query-interval
```

Parameter	Description
lan-delay	This command configures the Lan Delay configured for the router interface. This value ranges from 0 to 65535 milliseconds. The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the interface. It is used by upstream routers to find out the delayed time interval for a Join override message before pruning an interface. The no form of the command sets the default Lan Delay for the router per interface. Default value is 0.
message-interval	This command configures the frequency at which PIM Join/ Prune messages are transmitted on the PIM interface. This value ranges from 10 to 600 seconds. The same Join/ Prune message interval must be used on all the PIM routers in the PIM domain. If all the routers do not use the same timer interval, the performance of PIM Sparse can be adversely affected. The no form of the command resets the PIM Join/ Prune message to its default value: 60 seconds.
override-interval	This command configures the override interval configured for router interface. This value ranges from 0 to 65535 milliseconds. Override interval is the random amount of time delayed for sending override messages to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The no form of the command sets the default override interval for router interface: 0 milliseconds.
query-interval	This command enables PIM over an interface and configures the frequency at which PIM hello messages are transmitted on this interface. This value ranges from 1 to 18725 seconds. The query message informs the presence of a PIM router on the interface to the neighboring PIM routers.

	The no form of the command sets the default hello timer interval for this interface: 30 seconds.

This command can be executed in Interface Configuration Mode (VLAN/Router Port).

16.3.13 Show IP PIM

This command displays various PIM-related information.

```
show ip pim bsr [Component-Id <1-255>]
show ip pim component [ComponentId <1-255>]
show ip pim interface [{ Vlan <vlan_id> [df] | <interface-type><interface-id>
[df] | <IP-interface-type> <IP-interface-number> }]
show ip pim interface df
show ip pim mroute [bidir] [ {proxy | {compid<1-255> | <group-address> | <source-address> }
summary } ]
show ip pim neighbor [{ Vlan <vlan-id> | <interface-type> <interface-id> | <IP-interface-type>
<IP-interface-number>}]
show ip pim redundancy shadow-table
show ip pim redundancy state
show ip pim rp-candidate [ComponentId <1-255>] [bidir]
show ip pim rp-hash [<multicast_Group_address> <Group_mask>]
show ip pim rp-set [rp-address] [bidir]
show ip pim rp-static [ComponentId <1-255>] [bidir]
show ip pim rpf <source-address>
show ip pim thresholds
```

Parameter	Description
bsr	This command displays the BSR information. The component ID value ranges between 1 and 255.
component	This command displays the component information. The component ID value ranges between 1 and 255.
interface	This command displays the router's PIM interfaces. The information contains the list of Interface addresses, the mode of the interface, Designated Router on that interface, Hello Interval, Join/Prune Interval of the interface., bidirectional status , offer limit and offer interval.
interface df	This command displays the df states of all the PIM interfaces.
mroute	This command displays the PIM multicast information. Mroutes are multicast routing cache entries created by a user level mrouting daemon.
neighbor	This command displays the router's PIM neighbors' information. The information contains the Neighbor Address, the interface used to reach the PIM Neighbor, the Up time (the time since this neighbor became the neighbor of the local router), Expiry Time (the min. time remaining before this PIM neighbor will be aged out), LAN delay and Override interval.
redundancy	This command displays: • The shadow-table information for PIMv4 Route entries. • The status of PIM HA feature (enabled/disabled), status of active and standby PIM instance and status of dynamic bulk update.
rp-candidate	This command displays the candidate RP information. The information contains the Group addresses, the Group Mask and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.
rp-hash	This command displays the elected RP for the multicast group address with the mask length.
rp-set	This command displays the RP-set information. This information includes details of the Group Prefix, RP address, Hold time and Expiry Time.

rp-static	This command displays the static RP information. The component ID value ranges between 1 and 255.
rpf	This command displays the Reverse Path Forwarding (RPF) information for PIM module.
threshold	This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM (Sparse mode).

This command can be executed in User or in Privileged Mode.

17 STATIC ROUTING

17.1 IP Route

This command adds a static route. The Route defines the IP address or interface through which the destination can be reached.

The no form of this command deletes a static route.

```
ip route <prefix> <mask> {<next-hop> | Vlan <vlan-id> [<next-hop>] | <interface-type>
<interface-id> [<next-hop>] } [<distance(1-255)>] [private] [permanent] [name <nexthop-name>]
no ip route <prefix> <mask> {<next-hop> | Vlan <vlan-id> [<next-hop>] | <interface-type>
<interface-id> [<next-hop>] } [<distance(1-255)>] [private] [permanent] [name <nexthop-name>]
```

Parameter	Description
prefix	Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network.
mask	Configures the subnet mask for the IP address. This is a 32-bit number which is used to divide the IP address into network address and host address.
next-hop	Configures the IP address or IP alias of the next hop that can be used to reach that network.
vlan	Configures the static route for the specified VLAN.
interface-type	Interface Type
interafce-id	Interface Number
distance	Configures the Administrative distance for the specified next hop address or the interface. This value ranges from 1 to 255.
private	Sets the Private route
permanent	Sets the Permanent route.
name	Configures next hope name for the newly added static route.

This command can be executed in Global Configuration Mode.

17.2 IPv6 Route

This command adds a static IPv6 route. The Route defines the IP address or interface through which the destination can be reached.

The no form of this command deletes a static route.

```
ipv6 route <prefix> <prefix len> <NextHop> [<administrative distance>] [unicast]
no ipv6 route <prefix> <prefix len> <NextHop> [<administrative distance>] [unicast]
ipv6 route <prefix> <prefix len> <NextHop> vlan <vlan-id> [<administrative distance>] [{unicast
| anycast}]
no ipv6 route <prefix> <prefix len> <NextHop> vlan <vlan-id> [<administrative distance>]
[{unicast | anycast}]
ipv6 route <prefix> <prefix len> vlan <vlan-id> [<administrative distance>] [{unicast |
anycast}]
no ipv6 route <prefix> <prefix len> vlan <vlan-id> [<administrative distance>] [{unicast |
anycast}]
ipv6 route <prefix> <prefix len> {<interface-type> <interface-id> | <IP-interface-type> <IP-
interface-id>} [<administrative distance>] [unicast]
no ipv6 route <prefix> <prefix len> {<interface-type> <interface-id> | <IP-interface-type> <IP-
interface-id>} [<administrative distance>] [unicast]
```

Parameter	Description
prefix	Configures the IPv6 Prefix of the destination
NextHop	Configures the IPv6 prefix of the next hop that is used to reach the next destination network.
vlan	Configures the IPv6 static route for the specified VLAN.
interface-type	Interface Type
interafce-id	Interface Number
administrative distance	Configures the metric to reach the destination. This value ranges from 1 to 4294967295.
unicast	Configures the prefix type as Unicast.
anycast	Configures the prefix type as Anycast

This command can be executed in Global Configuration Mode.

17.3 Displaying Routing Information

The routing information can be shown with these commands:

```
show ip route
show ipv6 route
```

These commands can be executed in User or in Privileged Configuration Mode.

18 RIP CONFIGURATION

RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. RIP is classified by the IETF (Internet Engineering Task Force) as one of several internal gateway protocols.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers about the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count for determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet for a specified destination.

The RIP protocol can be configured either through CLI or in WEB on Routing → RIP page.

18.1 Router RIP

This command enables RIP protocol and enters the router configuration mode.

The no form of the command disables RIP on all interfaces.

Upon executing this command, the CLI changes its mode into router configuration mode

```
(config)# router rip
(config-router)#
```

This command can be executed in User or in Privileged Mode.

18.2 Network

This command enables RIP on an IP network for an unnumbered VLAN interface / router port. It configures a list of networks for the RIP routing process. RIP routing updates will be sent and received only through the specified interfaces on this network. If an interface's network is not specified, then the network will not be advertised in any RIP update.

The no form of the command disassociates RIP routing process with the specified IP network for an unnumbered VLAN interface / router port.

```
network <ip-address>[unnum {vlan <vlan-id>  | <iftype> <ifnum>}]
no network <ip-address> [unnum {vlan <vlan-id> | <iftype> <ifnum>}]
```

Parameter	Description
ip-address	Configures the IP network address of the interface that is to be associated with RIP routing process. The network IP address specified must not contain any subnet information. RIP routing updates will be sent and received only through interfaces on this network. The IP address should be same as that of the existing VLAN interface / router port.
vlan	VLAN ID
iftype ifnum	Interface type and Interface Number

This command can be executed in RIP Router Configuration Mode.

18.3 Neighbor

This command adds a trusted neighbor router with which routing information can be exchanged and from which RIP packets can be accepted. This command permits the point-to-point (non-broadcast) exchange of routing information. When used in combination with the passive-interface VLAN, router configuration command, routing information can be exchanged between a subset of routers and access servers. On a LAN multiple neighbor commands can be used to specify additional neighbors or peers.

The no form of the command deletes a trusted neighbor router.

```
neighbor <ip address>
no neighbor <ip address>
```

Parameter	Description
ip-address	IP address of neighbor router.

This command can be executed in RIP Router Configuration Mode.

18.4 Passive-Interface

This command suppresses the RIP routing updates on a specified VLAN interface in a defined or on a specified router port. It denotes that the RIP process runs in a passive VLAN interface / passive router port.

If the sending of routing updates is disabled on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The no form of the command restricts suppressing of RIP routing updates from an interface.

```
passive-interface {vlan <vlan-id > | <interface-type> <interface-id>}
no passive-interface {vlan <vlan-id > | <interface-type> <interface-id>}
```

Parameter	Description
vlan	VLAN ID
iftype ifnum	Interface type and Interface Number

This command can be executed in RIP Router Configuration Mode.

18.5 Redistribute

This command enables RIP to participate in Route Redistribution. When enabled, RIP starts advertising the routes learned by other protocols.

The no form of the command disables RIP to participate in Route Redistribution.

```
redistribute {all | connected | ospf | static} [route-map <string(20)>]
redistribute { isis } [{level-1 | level-2 | level-1-2}] [route-map <string(20)>]
```

Parameter	Description
all	Specifies that all routes have to be imported from the RIP. Redistributes all routes that are learnt into RIP process.
connected	Imports directly connected networks routes into RIP routing process.
ospf	Imports routes that are learnt by the OSPF process into RIP routing process.
static	Imports routes configured statically into RIP routing process.

isis	Imports routes that are learnt by ISIS into RIP routing process.
route-map	Specifies the name of the route-map in the list of route-maps. This value is a string with the maximum size as 20.

This command can be executed in RIP Router Configuration Mode.

18.6 Distance

command enables the administrative distance (that is, the metric to reach destination) of the routing protocol and sets the administrative distance value. The distance value ranges between 1 and 255.

The administrative distance can be enabled for only one route map. The distance should be disabled for the already assigned route map, if distance needs to be enabled for another route map.

The no form of the command disables the administrative distance.

```
distance <1-255> [route-map <name(1-20)>]
no distance [route-map <name(1-20)>]
```

This command can be executed in RIP Router Configuration Mode.

18.7 Auto-Summary

This command enables or disables the auto summarization of routes in RIP and restores the default behavior of automatic summarization of subnet routes into network-level routes.

```
auto-summary {enable | disable}
```

Parameter	Description
enable	Enables auto summarization feature in RIP, so that the summary routes are sent in regular updates for RIP.
disable	Disables auto summarization feature in RIP, so that either individual subnet route is sent or subnet routes are sent based on the specific aggregation configured over the interface.

This command can be executed in RIP Router Configuration Mode.

18.8 IP Split-Horizon

This command enables the split horizon updates for the RIP which prevents the routing loops in distance routing protocol, by prohibiting the router from advertising a route back onto the interface. The split horizon updates are applied in the response packets sent.

The no form of the command disables the split horizon updates.

```
ip split-horizon [poisson]
no ip split-horizon
```

Parameter	Description
poisson	Configures the split horizon with poisson reverse enabled. It's the default value.

This command can be executed in Interface Configuration Mode (VLAN / Router Port).

18.9 Version

This command sets the global version of RIP.

The no form of the command sets the RIP global version to its default value.

Defaults are 1 and 2.

```
version ( [1] [2])
no version
```

Parameter	Description
1	Sets global verison of RIP as 1. This implies that RIP updates aree sent/ received in compliance with RFC 1058.
2	Sets global verison of RIP as 2. This implies that only multicasting RIP updates are sent/ received.

This command can be executed in RIP Router Configuration Mode.

18.10 IP RIP Default Route Originate

This command sets the metric to be used for default route propagated over the VLAN interface / router port in a RIP update message and generates a default route into RIP. The metric value ranges between 1 and 15.

The no form of the command disables origination of default route over the interface.

```
ip rip default route originate <metric(1-15)>
no ip rip default route originate
```

This command can be executed in Interface Configuration Mode (VLAN / Router Port).

18.11 IP RIP Summary-Address

This command sets route aggregation over a VLAN interface / router port for all subnet routes that falls under the specified IP address and mask.

The no form of the command disables route aggregation with the specified IP address and mask.

```
ip rip summary-address <ip-address> <mask>
no ip rip summary-address <ip-address> <mask>
```

This command can be executed in Interface Configuration Mode (VLAN / Router Port).

18.12 IP RIP Default Route Install

This command installs the default route received in updates to the RIP database.

The no form of the command blocks the installation of default route received in updates to the RIP database.

```
ip rip default route install
no ip rip default route install
```

This command can be executed in Interface Configuration Mode (VLAN / Router Port).

18.13 Timers Basic

This command configures update, route age and garbage collection timers for the VLAN interface / router port.

The no form of the command sets update, route age and garbage collection timers to the default values.

```
timers basic <update-value (10-3600)> <routeage-value (30-500)> <garbage-value (120-180)>
no timers basic
```

Parameter	Description
update-value	Configures the time interval (in seconds) at which the RIP updates should be sent. This is the fundamental timing parameter of the routing protocol. This value ranges from 10 to 3600 seconds. Default: 30.
routeage-value	Configures the time (in seconds) after which the route entry is put into garbage collect (that is, marked as invalid). This value ranges from 30 to 500 seconds. Default: 180
garbage-value	Configures the time (in seconds) after which the route entry marked as invalid is deleted. The advertisements of this entry is set to INFINITY while sending to others. This value ranges from 120 to 180 seconds. Default: 120.

This command can be executed in Interface Configuration Mode (VLAN / Router Port).

18.14 RIP General Timers and Parameters

These commands configure various Timers and Parameters of RIP Protocol. The no version of a command restores default value.

```
ip rip retransmission { interval <timeout-value (5-10)> | retries <value (10-40)> }
no ip rip retransmit { interval | retries }
output-delay <milli-seconds (8-50)>
no output-delay
default-metric [ <value> ]
no default-metric [<short (1-16)>]
```

Parameter	Description
retransmission interval	Configures the timeout interval to be used to retransmit the update request packet or an unacknowledged update response packet. The packets are transmitted at the specified interval till a response is received or the maximum retries. This value ranges from 5 to 10. Default: 5
retransmission retries	Configures the maximum number of retransmissions of the update request and update response packets. This value ranges from 10 to 40. Default: 36.
output-delay	This command enables interpacket delay for RIP updates, where the delay is in milliseconds between packets in a multiple-packet RIP update. This interpacket delay feature helps in preventing the routing table from losing information due to flow of RIP update from high speed router to low speed router. The delay value ranges from 8 to 50 milliseconds.
default-metric	This command sets the default metric values to be used for redistributed routes for RIP, where the default metric to be used for the imported routes from RTM. The command is used in conjunction with the redistribute, router command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps in solving the problem of redistributing routes with incompatible metrics. The default metric provides a reasonable substitute and enables the redistribution to proceed further . The metric value ranges between 1 and 16. The no form of the command sets the metric used with redistributed routes to its default value: 3.

This command can be executed in RIP Router Configuration Mode.

18.15 Show IP RIP

This command displays IP RIP protocol database ,statistics or authentication related information.

```
show ip rip {database [<ip-address> <ip-mask>] | statistics | authentication}
```

Parameter	Description
database	Displays the RIP protocol database details for all RIP interface entry or for entry with the specified IP address and IP mask.
statistics	Displays the RIP statistics on the router.
authentication	Displays the authentication related information configured for the RIP Interface entry. The Authentication information include the Authentication Type, Authentication Key-ids configured & its associated lifetime values.

This command can be executed in User or in Privileged Mode.

19 VRRP CONFIGURATION

VRRP (Virtual Router Redundancy Protocol) is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP routers(s) on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the master router with the other routers acting as backups in case of the failure of the master router. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment.

VRRP protocol can be configured through CLI.

19.1 Router VRRP

This command enables VRRP globally in the router and enters into the VRRP Router Configuration Mode, which allows the user to execute all the commands which supports this mode.

The no form of the command disables VRRP in the router.

```
router vrrp
no router vrrp
```

This command can be executed in Global Configuration Mode.

19.2 Interface VRRP

This command enables VRRP for the specified interface and enters into the VRRP Interface Configuration Mode, which allows the user to execute all the commands which supports this mode.

The no form disables VRRP for the specified interface.

```
interface { vlan <vlan-id> | <interface-type> <interface-id> }
no interface { vlan <vlan-id> | <interface-type> <interface-id> }
```

Parameter	Description
vlan	Configures VLAN ID to be used for VRRP.
interface-type	Interface Type to be used for VRRP
interface-number	Interface number to be used for VRRP.

This command can be executed in VRRP Router Configuration Mode.

19.3 VRRP Address

This command sets the associated IPv4 or IPv6 addresses for the virtual router. On executing this command, the VRRP module starts the transition from ‘Initial’ state to either ‘Backup’ state or ‘Master’ state as per the election process on the specific interface.

The no form of the command deletes the associated IPv4 or IPv6 addresses for the virtual router.

```
vrrp <vrid(1-255)> ipv4 <ip_addr> [secondary]
no vrrp <vrid(1-255)> ipv4 <ip_addr> [secondary]
vrrp <vrid(1-255)> ipv6 <ip6_addr> [secondary]
no vrrp <vrid(1-255)> ipv6 <ip6_addr> [secondary]
```

Parameter	Description
vrid	Configures virtual router identifier (VRID) which is a number along with an interface to uniquely identify a virtual router on a given VRRP router. This value ranges from 1 to 255.
ipv4	Configures an IPv4 address for the specified virtual router ID.
ipv6	Configures an IPv6 address for the specified virtual router ID.
secondary	Configures the secondary IP address for the specified virtual router.

This command can be executed in VRRP Interface Configuration Mode.

19.4 VRRP Priority

This command sets the IPv4 or IPv6 priority for the virtual router.

The no form of the command sets the IPv4 or IPv6 priority for the virtual router to its default value.

```
vrrp <vrid(1-255)> [ ipv4 ] priority <priority(1-254)>
no vrrp <vrid(1-255)> [ ipv4 ] priority
vrrp <vrid(1-255)> ipv6 priority <priority(1-254)>
no vrrp <vrid(1-255)> ipv6 priority
```

Parameter	Description
vrid	Specifies a virtual router ID created for which the priority is to be set. This value ranges from 1 to 255.
ipv4	Sets the priority value for the IPv4 address assigned to the VRID.
ipv6	Sets the priority value for the IPv6 address assigned to the VRID.
priority	Sets the priority which is used for the virtual router master election process. Higher values implies higher priority. A priority of 255 is used for the router that owns the associated IP address(es). Default priority is 100.

This command can be executed in VRRP Interface Configuration Mode.

19.5 VRRP Preempt

This command enables the pre-emption of state change from either Backup to Master or vice versa based on the election process.

The no form of the command disables the preempt mode.

```
vrrp <vrid(1-255)> [ ipv4 ] preempt [ delay minimum <value(0-30)> ]
no vrrp <vrid(1-255)> [ ipv4 ] preempt
vrrp <vrid(1-255)> ipv6 preempt [ delay minimum <value(0-30)> ]
no vrrp <vrid(1-255)> ipv6 preempt
```

Parameter	Description
vrid	Specifies a virtual router ID created for which the preempt state change is to be enabled. This value ranges from 1 to 255.
ipv4	Sets pre-emption of state change for the IPv4 address assigned to the VRID.
ipv6	Sets pre-emption of state change for the IPv6 address assigned to the VRID.
delay minimum	Sets the number of seconds that the router will delay before issuing an advertisement claiming master ownership. This value ranges from 0 to 30.

	Default value is 0 and currently can't be changed.

This command can be executed in VRRP Interface Configuration Mode.

19.6 VRRP-Text-Authentication

This command sets the authentication type for the virtual router to simple password.

The no form of the command sets the authentication type for the virtual router to none

```
vrrp <vrid(1-255)> text-authentication <password>
no vrrp <vrid(1-255)> text-authentication
```

Parameter	Description
vrid	Configures a virtual router ID for which the authentication type is to be set. This value ranges from 1 to 255.
password	Sets the authentication password which is used to validate the incoming VRRP packets. The maximum value of this string is 8.

This command can be executed in VRRP Interface Configuration Mode.

19.7 VRRP Interval

The following command configure VRRP advertisement timer. The no version of a command restores default value.

```
vrrp <vrid(1-255)> timer [msec] <interval(1-255)secs>
no vrrp <vrid(1-255)> timer
```

Parameter	Description
vrid	Virtual Router ID. This value ranges from 1 to 255.
interval	Configures the time interval between successive advertisement messages in seconds. On expiry of the advertise timer, the Master sends advertisement packets to the Backup. This value ranges from 1 to 255 in seconds. Default: 1 second.

This command can be executed in VRRP Interface Configuration Mode.

19.8 Auth-Deprecate

This command enables or disables the Auth Deprecation flag.

```
auth-deprecate { enable | disable }
```

Parameter	Description
enable	Enables the AuthDeprecation flag. This is the default value
disable	Disables the AuthDeprecation flag.

This command can be executed in VRRP Router Configuration Mode.

19.9 VRRP Tracking Objects

The following commands operate with VRRP Tracking Objects. The no version of a command removes objects from a track.

```
track <group-index> interface { vlan <vlan _id> | <iftype> <ifnum> }
no track <group-index> interface { vlan <vlan_id> | <iftype> <ifnum> }
track <group-index> links <links-to-track(1-255)>
```

```
no track <group-index> links
```

Parameter	Description
interface	This command creates track group and adds an interface to the track group. The no form of this command deletes a track group and / or removes an interface from the track group.
links	This command configures number of links to track. The no form of this command resets the number of links to track.
group-index	Configures the track group for an interface.This value range from 1 to 4294967295.

This command can be executed in Global Configuration Mode.

19.10 VRRP-Version

This command sets the VRRP version in the router.

```
vrrp version { v2 | v2-v3 | v3 }
```

Parameter	Description
v2	Sets the VRRP version in the router as Version 2. This is the default version.
v2-v3	Sets the VRRP version in the router as Version 2 and Version 3.
v3	Sets the VRRP version in the router Version 3.

This command can be executed in VRRP Router Configuration Mode.

19.11 VRRP-Accept-Mode

This command enables or disables accept mode status for the specified interface.

```
vrrp <vrid(1-255)> [ ipv4 ] accept-mode { enable | disable }
vrrp <vrid(1-255)> ipv6 accept-mode { enable | disable }
```

Parameter	Description
vrid	Configures a virtual router ID for which the priority is to be set. This value ranges from 1 to 255.
ipv4	Configures an IPv4 address to be assigned to the VRID.
ipv6	Configures an IPv6 address to be assigned to the VRID.

This command can be executed in VRRP Interface Configuration Mode.

19.12 VRRP Tracking Group

This command enables or disables accept mode status for the specified interface.

```
vrrp <vrid(1-255)> [ ipv4 ] track <group-index> decrement <integer(1-254)>
no vrrp <vrid(1-255)> [ ipv4 ] track
vrrp <vrid(1-255)> ipv6 track <group-index> decrement <integer(1-254)>
no vrrp <vrid(1-255)> ipv6 track
```

Parameter	Description
vrid	Configures a virtual router ID for which the priority is to be set. This value ranges from 1 to 255.

ipv4	Configures an IPv4 address to be assigned to the VRID.
ipv6	Configures an IPv6 address to be assigned to the VRID.
track	Specifies the track group for an interface.This value range from 1 to 4294967295.
decrement	Configures the decrement priority for an interface.This value is from 1 to 254.

This command can be executed in VRRP Interface Configuration Mode.

19.13 Show VRRP

This command displays various VRRP-related parameters.

```
show vrrp [interface { vlan <VlanId > | <interface-type> <interface-id>  } <VrId(1-255)>]
[{brief|detail |statistics}]
show vrrp interface [{ vlan <vlan-id > | <interface-type> <interface-id>}] [{brief|detail
|statistics}]
show track
```

Parameter	Description
vlan	Displays the VRRP status information for the specified VLAN.
interface-type	Inetrface Type.
intercace-id	Interface Number.
VrId	Displays the VRID which is a number along with an interface to uniquely identify a virtual router on a given VRRP router.
brief	Displays the brief VRRP status information.
detail	Displays the detailed VRRP status information.
statistics	Displays the statistical information for the VRRP.
track	Displays VRRP track group information.

This command can be executed in User or in Privileged Mode.

20 OSPF CONFIGURATION

OSPF (Open Shortest Path First) protocol, is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they result in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes a network more stable.

The OSPF routing protocol can be configured either through CLI, or in WEB on Routing → OSPF page.

20.1 Router OSPF

This command enables OSPF routing process and enters into the OSPF Router Configuration Mode, which allows the user to execute all commands supporting this Mode.

The no form of this command disables the OSPF Router Admin Status to terminate the OSPF process.

```
router ospf
no router ospf
```

This command can be executed in Global Configuration Mode.

20.2 Router-ID

This command sets the router-id for the OSPF process. The router ID is set to an IP address of a loopback interface if it is configured. An arbitrary value for the ip-address for each router can be configured; however, each router ID must be unique. To ensure uniqueness, the router-id must match with one of the router's IP interface addresses.

The no form of this command resets the configured router-id and dynamically select least interface ip as router-id for OSPF process

```
router-id <router ip address>
no router-id
```

This command can be executed in OSPF Router Configuration Mode.

20.3 Area-Virtual-Link

This command defines an OSPF virtual link and its related parameter. In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link. Hello-interval and dead-interval values must be the same for all routers and access servers on a specific network.

The no form of removes an OSPF virtual link.

```
area <area-id> virtual-link <router-id> [authentication { simple |message-digest | sha-1 | sha-
224 | sha-256 | sha384 | sha-512 | null}] [hello-interval <value (1-65535)>] [retransmit-
interval <value (1-3600)>] [transmit-delay <value (1-3600)>] [dead-interval <value>]
[{authentication-key <key (8)> | message-digest-key <Key-id (0-255)> {md5 | sha-1 | sha-224 |
sha-256 | sha-384 | sha-512} <key (16)>}]
no area <area-id> virtual-link <router-id> [authentication] [hello-interval] [retransmit-
interval] [transmit-delay] [dead-interval] [{authentication-key | message-digest-key <Key-id
(0-255)>}]
```

```
area <area-id> virtual-link <router-id> key <Key-ID (0-255)> start-accept <DD-MON-YEAR,HH:MM>
area <area-id> virtual-link <router-id> key <Key-ID (0-255)> stop-accept <DD-MON-YEAR,HH:MM>
area <area-id> virtual-link <router-id> key <Key-ID (0-255)> start-generate <DD-MON-YEAR,HH:MM>
area <area-id> virtual-link <router-id> key <Key-ID (0-255)> stop-generate <DD-MON-YEAR,HH:MM>
```

Parameter	Description
area-id	Configures the area ID assigned to the transit area for the virtual link. The Transit Area that the Virtual Link traverses. It is specified as an IP address This can be either a decimal value or a valid IP address.
router-id	Configures the router ID of the virtual neighbor.
authentication	Configures the authentication type. The list contains: • simple – Sets the simple password authentication mechanism. • message-digest – Sets the message digest authentication mechanism. • sha-1 - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes. • sha-224 - Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes. • sha-256 - Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes. • sha-384 - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes. • sha-512 - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes. • null – Sets the no password authentication.
hello-interval	Sets the interval between hello packets that the software sends on the OSPF virtual link interface. This value ranges from 1 to 65535 in seconds.
retransmit-interval	Sets the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface. This value ranges from 1 to 3600 in seconds.
transmit-delay	Sets the time in which the router will stop using this key for packets generation. Estimated time required to send a link-state update packet on the interface. Integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. This value ranges from 1 to 3600 in seconds.
dead-interval	Sets the interval at which hello packets must not be seen before its neighbors declare the router down. As with the hello interval, this value must be the same for all routers and access servers attached to a common network. This value ranges from 1 to 65535 seconds.
authentication-key	Identifies the secret key used to create the message digest appended to the OSPF packet Password to be used by neighboring routers. This string acts as a key that will allow the authentication procedure to generate or verify the authentication field in the OSPF header. This is a sting with maximum string size 8.
message-digest-key	Enables Message Digest 5 (MD5) authentication on the area specified by the area-id. This value ranges from 0 to 255.

md5	Configures the authentication type as Message Digest 5 (MD5) authentication.
sha-1	Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
sha-224	Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes.
sha-256	Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
sha-384	Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.
sha-512	Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.
key	Configures the cryptographic key value which is used used to create the message digest appended to the OSPF packet. All neighboring routers on the same network must have the same key identifier and key to route OSPF traffic. This is a sting with maximum string size 16.
key start-accept	This command configures the time the router starts accepting packets that is created with the configured key id.
key stop-accept	This command configures the time when the router stops accepting OSPF packets created by using the configured key-id.
key start-generate	This command configures the time when the switch starts generating ospf packets with configured key id on the switch.
key stop-generate	This command configures the time when the switch starts generating ospf packets with configured key id on the switch.

This command can be executed in OSPF Router Configuration Mode.

20.4 Area-Stub

This command specifies an area as a stub area and other parameters related to that area. This command is configured on all routers and access servers in the stub area.

The no form of the command removes an area or converts stub/nssa to normal area.

```
area <area-id> stub [no-summary]
no area <area-id> [{ stub [no-summary] | nssa [no-redistribution] [Default-information-
originate [metric<value>] [metric-type <Type(1-3)> ]][no-summary]}]
```

Parameter	Description
area-id	Configures the identifier of the area associated with the OSPF address range for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
no-summary	Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area by neither originating nor propagating summary LSA into the stub area.
nssa	Configures the area as Not-So-Stubby Area (NSSA). • no-redistribution - Disables redistribution of routes from the given protocol into OSPF.

Default-information originate	Configures default route into OSPF. • metric <value> - Configures metric related configurations applied to the route before it is advertised into the OSPF domain. This value ranges from 0 to 16777215. • metric-type <Type(1-3)> - Configures the metric type applied to the route before it is advertised into the OSPF domain. This value ranges from 1 to 3.
no-summary	Allows an area to be a not-so-stubby area but not have summary routes injected into it.

This command can be executed in OSPF Router Configuration Mode.

20.5 Area-NSSA

This command configures a particular area as not-so-stubby area (NSSA).

```
area <area-id> nssa [{ no-summary | default-information-originate [metric <value (0-16777215)>]
[metric-type <Type(1-3)>] [tos <tos value (0-30)>] [no-redistribution] }]
no area <area-id> [{ stub [no-summary] | nssa [no-redistribution] [Default-information-
originate [metric<value>] [metric-type <Type(1-3)> ]][no-summary]}]
```

Parameter	Description
area-id	Configures the identifier of the area associated with the OSPF address range for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
no-summary	Allows an area to be a not-so-stubby area but not have summary routes injected into it.
Default-information-originate	Configures the default route into OSPF and used to generate a Type 7 default into the NSSA area.
metric	The Metric value applied to the route before it is advertised into the OSPF domain. This value ranges from 0 to 16777215.
metric-type	The Metric Type applied to the route before it is advertised into the OSPF domain. This value ranges from 1 to 3.
tos	Type of Service of the route being configured. This value ranges from 0 to 30. It can be configured only if the code is compiled with TOS Support.
no-redistribution	Disables redistribution of routes from the given protocol into OSPF.

This command can be executed in OSPF Router Configuration Mode.

20.6 Area-Default Cost

This command specifies a cost for the default summary route sent into a stub or NSSA. This command is used only on an Area Border Router (ABR) attached to a stub or NSSA. This command provides the metric for the summary default route generated by the ABR into the stub area.

The no form of the command removes the assigned default route cost.

```
area <area-id> default-cost <cost> [tos <tos value(0-30)>]
no area <area-id> default-cost [tos <tos value (0-30)>]
```

Parameter	Description
area-id	Configures the identifier for the stub or NSSA. The identifier can be specified as either a decimal value or as an IP address.

default-cost	Configures the cost for the default summary route used for a stub or NSSA. A default cost can be defined only for a valid area. This value ranges from 0 to 16777215.
tos	Configures the Type of Service of the route being configured. This value ranges from 0 to 30. It can be configured only if the code is compiled with TOS Support.

This command can be executed in OSPF Router Configuration Mode.

20.7 Area-Stability Interval

This command configures the Stability interval for NSSA where the Information describing the configured parameters and cumulative statistics of one of the router's attached areas.

The no form of the command configures default Stability interval for NSSA.

```
area <area-id> stability-interval <Interval-Value (0 - 0x7fffffff)>
no area <area-id> stability-interval
```

Parameter	Description
area-id	Configures the area id associated with the OSPF address range (ipv4 address). Area ID 0.0.0.0 is used for the OSPF backbone.
Interval-Value	Configures the time interval after an elected translator determines its services are no longer required, that it must continue to perform its translation duties. The interval value ranges between 0-0x7fffffff in seconds.The OSPF Sequence Number is a 32 bit signed integer. It starts with the value '80000001'h, -- or -'7FFFFFFF', and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative

This command can be executed in OSPF Router Configuration Mode.

20.8 Area-Translation-Role

This command configures the translation role for the NSSA.

The no form of the command configures the default translation role for the NSSA.

```
area  <area-id> translation-role { always | candidate }
no area  <area-id> translation-role
```

Parameter	Description
area-id	Configures the area id associated with the OSPF address range. It is specified as an IP address.
translation-role	Configures Aan NSSA Border router's ability to perform NSSA Translation of Type-7 LSAs to Type-5 LSAs.The options are : • always – Sets translator role where the Type-7 LSAs are always translated into Type-5 LSAs. Type-5 LSAs- Originated by AS (Autonomous system) boundary routers, and flooded through-out the AS. Each AS-external-LSA describes a route to a destination in another Autonomous System. default routes for the AS can also be described by AS-external-LSAs. • candidate – Sets translator role where an NSSA border router participates in the translator election process.

This command can be executed in OSPF Router Configuration Mode.

20.9 Area-Range

This command consolidates and summarizes routes at an area boundary which is used only with Area Border Routers (ABRs). The result is that a single summary route is advertised to other areas by the ABR.

The no form of the command deletes the Summary Address.

```
area <AreaId> range <Network> <Mask> {summary | Type7} [{advertise | not-advertise}] [tag
<value>]
no area <AreaId> range <Network> <Mask> [type7] [{advertise | not-advertise}] [tag <tag-value>]
[cost <value>]
```

Parameter	Description
area-id	Configures the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
Network	Configures the IP address of the network indicated by the range.
Mask	Configures the subnet mask that pertains to the range. The mask indicates the range of addresses being described by the particular route. For example, a summary-LSA for the destination 128.185.0.0 with a mask of 0xffff0000 actually is describing a single route to the collection of destinations 128.185.0.0 - 128.185.255.255.
summary	Sets the LSA type as summary LSA.
Type7	Sets the LSA type as Type-7 LSA.
advertise	Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA). When associated area Id is 0.0.0.0, aggregated Type-5 are generated. For associated other than 0.0.0.0 aggregated Type-7 is generated in NSSA x.x.x.x.
not-advertise	Sets the address range status to Not Advertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks When associated area Id is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. For associated area Id x.x.x.xother than 0.0.0.0, Type-7 are not generated in NSSA x.x.x.x for the specified range.
tag	Configures the Tag Type which describes whether Tags will be generated automatically or manually configured. This value ranges from 0 to 2147483647.
cost	Configures the route path cost.

This command can be executed in OSPF Router Configuration Mode.

20.10 ABR-Type

This command sets the Alternative ABR Type.

The no form of the command resets the configured Alternative ABR Type.

```
abr-type { standard | cisco | ibm }
no abr-type
```

Parameter	Description
standard	Configures the Standard ABR type as defined in RFC 2328.
cisco	Configures the CISCO ABR type as defined in RFC 3509

ibm	Configures the IBM ABR type as defined in RFC 3509

This command can be executed in OSPF Router Configuration Mode.

20.11 Neighbor

This command specifies a neighbor router and its priority. This command configures the Router ID of the OSPF routers interconnecting to non-broadcast networks.

The no form of this command removes the neighbor and resets the neighbor priority to its default value.

```
neighbor <neighbor-id> [priority  <priority value (0-255)>] [poll-interval seconds] [cost
number] [database-filter all]
no neighbor <neighbor-id> [priority] [poll-interval seconds]    [cost number] [database-filter
all out]
```

Parameter	Description
neighbor-id	Configures the Neighbor router ID based on which the priority of the neighbor is defined.
priority	Indicates a number value that specifies the router priority and the priority of the nonbroadcast neighbor router associated with the specified IP address. The router with the highest priority becomes the designated router. This value ranges from 0 to 255.The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network.
poll-interval seconds	Configures the poll interval between the Hello packets sent to an inactive non-broadcast multi-access neighbor.
cost number	Configure route path cost value.
database-filter all	Configures database filter.

This command can be executed in OSPF Router Configuration Mode.

20.12 Default-Information Originate Always

This command enables generation of a default external route into an OSPF routing domain and other parameters related to that area.

The no form of the command disables generation of a default external route into an OSPF routing domain.

```
default-information originate always [metric <metric-value (0-16777215)>] [metric-type <type
(1-2)>]
no default-information originate always [metric <metric-value (0-16777215)>] [metric-type <type
(1-2)>]
```

Parameter	Description
neighbor-id	always - Advertises the default route always regardless of whether the software has a default route.
metric	Sets the Metric value applied to the route before it is advertised into the OSPF Domain Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 1. The value used is specific to the protocol.This value ranges from 0 to 16777215.
metric-type	Sets the Metric Type applied to the route before it is advertised into the OSPF Domain External link type associated with the default route

	advertised into the OSPF routing domain. It can be one of the following values: • 1 - Sets Type 1 external route • 2 - Sets Type 2 external route

This command can be executed in OSPF Router Configuration Mode.

20.13 ASBR Router

This command specifies this router as ASBR. Routers that act as gateways (redistribution) between OSPF and other routing protocols (IGRP, EIGRP, RIP, BGP, Static) or other instances of the OSPF routing process are called autonomous system boundary router (ASBR).

The no form of the command disables this router as ASBR.

```
ASBR Router
no ASBR Router
```

This command can be executed in OSPF Router Configuration Mode.

20.14 Summary-Address

This command creates aggregate addresses for OSPF and helps in reducing the size of the routing table.

The no form of the command deletes the External Summary Address.

```
summary-address <Network> <Mask> <AreaId> [{allowAll | denyAll |  advertise | not-advertise}]
[Translation {enabled | disabled}][tag tag-value]
no summary-address <Network> <Mask> <AreaId> [not-advertise] [tag tag-value]
```

Parameter	Description
Network	Configures the IP address of the Net indicated by the range.
Mask	Configures the subnet mask that pertains to the range.
AreaId	Configures the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address. The Area Id should be of backbone area or NSSA area.
allowAll	Configures allowAll option and sets associated areaId as 0.0.0.0 which generates the aggregated Type-5 for the specified range. In addition aggregated Type-7 are generated in all attached NSSA, for the specified rangeThis parameter is valid only for areaId 0.0.0.0.
denyAll	Configures denyAll in which neither Type-5 nor Type-7 will be generated for the specified range. This parameter is valid only for areaId 0.0.0.0.
advertise	Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA). When associated area Id is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated areaId is x.x.x.x (other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x.
not-advertise	Sets the address range status to NotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks When associated area Id is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While if associated area Id is x.x.x.x(other than 0.0.0.0), Type-7 are not generated in NSSA x.x.x.x for the specified range. This parameter is currently not supported in the no form of the command.

Translation	Indicates how an NSSA Border router is performing NSSA translation of Type-7 to into Type-5 LSAs. • enabled – Sets P Bit in the generated Type-7 LSA. • disabled - Clears P Bit in the generated Type-7 LSA.
tag tag-value	Configures the tag option for OSPF.This parameter is currently not supported.

This command can be executed in OSPF Router Configuration Mode.

20.15 Redistribute

This command configures the protocol from which the routes have to be redistributed into OSPF and advertises the routes learned by other protocols.

The no form of the command disables redistribution of routes from the given protocol

```
redistribute {static | connected | rip | all} [route-map <name(1-20)>] [metr
ic <mertic_value(0-16777214)>] [metric-type 1-2]
no redistribute {static | connected | rip | all} [route-map <name(1-20)>] [metr
ic <mertic_value(0-16777214)>] [metric-type 1-2]
```

Parameter	Description
static	Redistributes routes, configured statically in the OSPF routing process.
connected	Redistributes directly connected networks routes into OSPF routing process.
rip	Redistributes routes that are learnt by the RIP process into OSPF routing process.
all	Imports all routes learnt in the OSPF routing process.
route-map	Identifies the specified route-map in the list of route-maps. This is a string with maximum string size 20.
metric	Configures the metric values for the routes to be redistributed into ospf. This value ranges from 0 to 16777214.
metric-type	Configures the metric type applied to the routes to be redistributed. This value ranges from 1 to 2.

This command can be executed in OSPF Router Configuration Mode.

20.16 Distribute-list Route-Map In

This command enables inbound filtering for routes and defines the conditions for distributing the routes from one routing protocol to another.

The no form of the command disables inbound filtering for the routes.

```
distribute-list route-map <name(1-20)> in
no distribute-list route-map <name(1-20)> in
```

Parameter	Description
name	Configures the name of the Route Map for which filtering should be enabled. Only one route map can be set for inbound routes. Another route map can be assigned, only if the already associated route map is disassociated. This value is a string with maximum string size 20.

This command can be executed in OSPF Router Configuration Mode.

20.17 REDIST-Config

This command configures the information to be applied to routes learnt from RTM.

The no form of the command deletes the information applied to routes learnt from RTM.

```
redist-config <Network> <Mask> [metric-value <metric (1 - 16777215)>] [metric-type {asExttype1
| asExttype2}]  [tag <tag-value>}
no redist-config <Network> <Mask>
```

Parameter	Description
Network	Confgures the IP Address of the Destination route.
Mask	Configures the Mask of the Destination route.
metric-value	Configures the Metric value applied to the route before it is advertised into the OSPF Domain. This value ranges from 1 to 16777215.
metric-type	Configures the Metric Type applied to the route before it is advertised into the OSPF Domain. The list options are: • asExttype1 – Sets the metric type as AS external type 1. • asExttype2 - Sets the metric type as AS external type 2.
tag	Configures theTag Type describes whether Tags will be automatically generated or will be manually configured. This value ranges from 0 to 4294967295. This is not used by OSPF protocol itself. It may be used to communicate information between AS boundary routers. The precise nature of this information is outside the scope of OSPF. If tags are manually configured, the futospfRRDRouteTag MIB has to be set with the Tag value needed. To execute this command with the tag option, the router must to set as ASBR.

This command can be executed in OSPF Router Configuration Mode.

20.18 Capability Opaque

This command enables the capability of storing opaque LSAs.

The no form of the command disables the opaque capability. This is the default value.

```
capability opaque
no capability opaque
```

This command can be executed in OSPF Router Configuration Mode.

20.19 NSF IETF Restart

This command configures graceful restart parameters. The no version of this command deactivates the feature.

```
nsf ietf restart-support [plannedOnly]
no nsf ietf restart-support
nsf ietf restart-interval <grace period(1-1800)>
no nsf ietf restart-interval
nsf ietf restart-reason [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]
```

Parameter	Description
restart-support [plannedOnly]	This command enables the graceful restart support in OSPF router. Graceful restart support is provided for both unplanned and planned restart, if the command is executed without any option. The graceful restart mechanism allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a

	processor switch over. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. The no form of the command disables the graceful restart support. • plannedOnly - Configures planned only graceful restart mechanism in the OSPF router.
restart-interval	This command configures the OSPF graceful restart timeout interval. This value specifies the graceful restart interval, in seconds, during which the restarting router has to reacquire OSPF neighbors that are fully operational prior to the graceful restart. This value ranges from 1 to 1800 seconds. The value is provided as an intimation of the grace period to all neighbors. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. The no form of the command resets the interval to default value. Default value: 120 seconds.
restart-reason	This command configures the reason for graceful restart in the OSPF router. The reason for restart can be software upgrade, scheduled restart or switch to redundant router. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. • unknown - Configures the system to restart due to unplanned events (such as restarting after a crash). • softwareRestart - Configures the system to restart due to software restart. • swReloadUpgrade - Configures the system to restart due to reloading / upgrading of software. • switchToRedundant - Configures the system to restart due to switchover to a switchover to a redundant support processor.

This command can be executed in OSPF Router Configuration Mode.

20.20 NSF IETF Helper

This command configures helper support parameters. The no version of this command deactivates the feature.

```
nsf ietf helper-support [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]
no nsf ietf helper-support [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]
nsf ietf helper gracetimelimit <gracelimit period(0-1800)>
nsf ietf helper strict-lsa-checking
no nsf ietf helper strict-lsa-checking
```

Parameter	Description
helper-support	This command enables the helper support. The helper support is enabled for all the options, if the command is executed without any option. The helper support can be enabled for more than one option, one after the other. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. The no form of the command disables the helper support. The helper support is disabled for all the options, if the command is executed without any option. • unknown - Configures helper support for restarting of system due to unplanned events (such as restarting after a crash).

	• softwareRestart - Configures helper support for restarting of system due to restart of software. • swReloadUpgrade - Configures helper support for restarting of system due to reload or upgrade of software. • switchToRedundant - Configures helper support for restarting of system due to switchover to a redundant support processor.
gracetimelimit	This command configures the grace period till which the OSPF router acts as Helper. During this period, the router advertises that the restarting router is active and is in FULL state. This value ranges from 0 to 1800 seconds. The value is provided as an intimation of the restart period to the neighbors that do not support graceful restart or that are connected using multipoint interfaces.
strict-lsa-checking	This command enables the strict LSA check option in helper. The strict LSA check option allows the helper to terminate the graceful restart, once a changed LSA that causes flooding during the restart process is detected. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent. The no form of the command disables the strict LSA check option in helper.

This command can be executed in OSPF Router Configuration Mode.

20.21 NSF IETF Grace

This command configures Grace parameters. The no version of this command deactivates the feature.

```
nsf ietf grace lsa ack required
no nsf ietf grace lsa ack required
nsf ietf grlsa retrans count <grlsacout (0-180)>
```

Parameter	Description
lsa ack required	This command enables Grace Ack Required state in restarter. The GraceLSAs sent by the router are expected to be acknowledged by peers, if the Grace Ack Required state is enabled. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent The no form of the command disables the Grace Ack Required state in restarter.
retrans count	This command configures the maximum number of retransmissions for unacknowledged GraceLSA. This value ranges from 0 to 180. Default: 2.

This command can be executed in OSPF Router Configuration Mode.

20.22 Distance

This command updates the routes filtered via route-map at IP routing layer . The distance value (i.e. the preference value) ranges between 1 and 255.

The administrative distance (route preference value) can be updated for routes filtered via only one route map. The distance (route preference) should be disassociated for the already associated route map, if distance needs to be associated for another route map.

The no form of the command disables the administrative distance(route preference).

```
distance <1-255> [route-map <name(1-20)>]
no distance [route-map <name(1-20)>]
```

Parameter	Description
route-map	Configures the name of the Route Map for which the distance value should be enabled and set. This value is a string with maximum string size 20.

This command can be executed in OSPF Router Configuration Mode.

20.23 Route-Calculation Staggering

This command configures Route Calculation Staggering feature and its timing parameter. The no version of this command removes this feature.

```
route-calculation staggering
no route-calculation staggering
route-calculation staggering-interval <milli-seconds (1000-2147483647)>
```

Parameter	Description
staggering	This command enables OSPF route calculation staggering feature and also sets the staggering interval to the last configured value. This feature staggers the OSPF route calculation at regular intervals for processing neighbor keep alive and other OSPF operations. The no form of the command disables OSPF route calculation staggering and removes the staggering interval.
staggering-interval	This command configures the OSPF route calculation staggering interval (in milliseconds). This value represents the time after which the route calculation is suspended for doing other OSPF operations. This value ranges from 1000 to 2147483647 milliseconds. Default: 10000 miliseconds.

This command can be executed in OSPF Router Configuration Mode.

20.24 Network

This command defines the interfaces on which OSPF runs and the area ID for those interfaces. When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists. There is no limit to the number of network commands that can be used on the router. The IP address for the entry should be same as that of the configured interface.

The no form of the command disables OSPF routing for interfaces defined and to remove the area ID of that interface.

When OSPF routing is enabled using the “network” command, the session established is properly mapped with the interface only if the interface administrative status is up. This is because to enable OSPF in an interface, both IP address and interface index are used.

```
network <Network number> area <area-id> [unnum {Vlan <vlan-id> | <interface-type> <interface-
num>}]
no network <Network number> area <area-id> [unnum {Vlan <vlan-id> | <interface-type>
<interface-num>}]
```

Parameter	Description
network number	Configures the Network type for the interfaces.
area-id	Configures the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
unnum	Configures the Network type for the specified VLAN ID. This value ranges from 1 to 4094.

interface-type	Configures the Interface Type
interface-num	Interface Number

This command can be executed in OSPF Router Configuration Mode.

20.25 Set NSSA ASBR-Default-Route Translator

This command enables/disables setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR.

```
set nssa asbr-default-route translator { enable | disable }
```

Parameter	Description
enable	Sets P-Bit in the generated Type-7 default LSA, when nssa absr is set to enabled.
disable	Clears P-Bit in the generated default LAS, when nssa absr is set to disabled.

This command can be executed in OSPF Router Configuration Mode.

20.26 Passive-Interface

This command suppresses routing updates on an interface and makes the interface passive.

The no form of the command enables routing updates on an interface.

```
passive-interface {vlan <vlan-id> | <interface-type> <interface-id> }
no passive-interface {vlan <vlan-id> | <interface-type> <interface-id> }
passive-interface default
no passive-interface default
```

Parameter	Description
vlan	Configures the VLAN ID as passive interafce. This value ranges from 1 to 4094.
interface-type	Configures the Interface Type
interface-num	Interface Number
default	This command suppresses routing updates on all interfaces and makes the passive interface to default. All the OSPF interfaces created after the execution of this command will be passive. This is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces. The no form of the command enables routing updates on all interfaces.

This command can be executed in OSPF Router Configuration Mode.

20.27 OSPF Interface-Related Parameters and Timers

These commands configure various OSPF Interface-related parameters and Timers. The no version of a command restores default value.

```
ip ospf demand-circuit
no ip ospf demand-circuit
ip ospf retransmit-interval <seconds (1 - 3600)>
no ip ospf retransmit-interval
ip ospf transmit-delay <seconds (1 - 3600)>
no ip ospf transmit-delay
ip ospf priority <value (0 - 255)>
no ip ospf priority
```

```
ip ospf hello-interval <seconds (1 - 65535)>
no ip ospf hello-interval
ip ospf dead-interval <seconds (1-65535)>
no ip ospf dead-interval
ip ospf cost <cost (1-65535)> [tos <tos value (0-30)>]
no ip ospf cost [tos <tos value (0-30)>]
ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}
no ip ospf network
```

Parameter	Description
demand-circuit	This command configures OSPF to treat the interface as an OSPF demand circuit. On point-to-point interfaces, only one end of the demand circuit must be configured. This command allows the underlying data link layer to be closed when the topology is stable. It indicates whether Demand OSPF procedures (hello suppression to FULL neighbors and setting the DoNotAge flag on prorogated LSAs) must be performed on this interface On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command executes only if OSPF routing process is enabled. The no form of the command removes the demand circuit designation from the interface.
retransmit-interval	This command specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. This value ranges from 1 to 3600. This value is also used while retransmitting database description and link-state request packets. The no form of the command uses the default time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. Default is 5 seconds.
transmit-delay	This command sets the estimated time(in seconds) it requires to transmit a link state update packet on the interface. This value ranges from 1 to 3600. Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission. The no form of the command sets the default estimated time it takes to transmit a link state update packet on the interface. Default is 1 second.
priority	This command sets the router priority which helps determine the designated router for this network. When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence The number value that specifies the priority of the router ranges is from 0 to 255. When two routers attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. The no form of the command sets default value for router priority. Default is 1.
hello-interval	This command specifies the interval (in seconds) between hello packets sent on the interface. This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected. This value ranges from 1 to 65535. This value must be the same for all routers attached to a common network. The no form of the command sets default value for, interval between hello packets sent on the interface. Default: 10 seconds.

dead-interval	This command sets the interval (in seconds) at which hello packets must not be seen before neighbors declare the router down. The interval is advertised in router hello packets. This value ranges from 1 to 65535. The no form of the command sets default value for the interval at which hello packets must not be seen before neighbors declare the router down. This value must be the same for all routers and access servers on a specific network.
cost	This command explicitly specifies the cost of sending a packet on an interface. The link-state metric is advertised as the link cost in the router link advertisement. The no form of the command resets the path cost to the default value. In general, the path cost is calculated using the following formula: • 108 / bandwidth Using this formula, the default path costs are calculated • Example: 56-kbps serial link-Default cost is 1785 • Ethernet-Default cost is 10 <cost (1-65535)> - Configures the Type 1 external metrics which is expressed in the same units as OSPF interface cost, that is in terms of the OSPF link state metric. This value ranges from 1 to 65535. tos <tos value (0-30)> - Configures the type of Service of the route being configured. This value ranges from 0 to 30.
network	This command configures the OSPF network type to a type other than the default for a given media and configures broadcast networks as NBMA networks. Each pair of routers on a broadcast network is assumed to be able to communicate directly. An Ethernet is an example of a broadcast network. A 56Kb serial line is an example of a point-to-point network. The no form of the command sets the OSPF network type to the default type. • broadcast - Configures the broadcast networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast) • non-broadcast - Configures the non broadcast networks supporting many (more than two) routers, but having no broadcast capability Sets the network type to nonbroadcast multiaccess (NBMA). • point-to-multipoint - Sets the network type to point-to-multipoint and treats the non-broadcast network as a collection of point-to-point links • point-to-point - Sets the network type to point-to-point that joins a single pair of routers

This command can be executed in Interface configuration Mode (VLAN interface / Router port).

20.28 IP OSPF Authentication

These commands configure Authentication Mechanism for OSPF. The no version of a command removes authentication.

```
ip ospf authentication-key <password (8)>
no ip ospf authentication-key
```

```
ip ospf authentication {message-digest | sha-1 | sha-224 | sha-256 | sha-384 | sha-512 | null |
simple}
no ip ospf authentication
ip ospf message-digest-key <Key-ID (0-255)> [{ md5 | sha-1 | sha-224 | sha-256 | sha-384 | sha-
512}]  <Key (16)>
no ip ospf message-digest-key <Key-ID (0-255)>
```

Parameter	Description
authentication-key <password (8)>	This command specifies a password to be used by neighboring routers that are using the OSPF simple password authentication. The password created by this command is used as a key that is inserted directly into the OSPF header when the routing protocol packets are originated. The size of the password is 8 bytes. The password string can contain from 1 to 8 uppercase and lowercase alphanumeric characters. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information. The no form of the command removes a previously assigned OSPF password.
authentication	This command specifies the authentication type for an interface. The no form of the command removes the authentication type for an interface and sets it to NULL authentication
message-digest-key	This command enables OSPF MD5 authentication. One key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The no form of the command removes an old MD5 key. • Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a "message digest" that gets appended to the packet • Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

This command can be executed in Interface configuration Mode (VLAN interface / Router port).

20.29 Show IP OSPF

This command displays various IP OSPF-related parameters.

```
show ip ospf
show ip ospf [area-id] database {asbr-summary | external | network | nssa-external | opaque-
area | opaque-as | opaque-link | router | summary} [link-state-id] [{adv-router <ip-address> |
self-originate}]
show ip ospf [area-id] database [{database-summary | self-originate | adv-router <ip-address>}]
show ip ospf border-routers
show ip ospf interface [{vlan <vlan-id> | <interface-type> <interface-id>}]
show ip ospf neighbor [{vlan <vlan-id> | <interface-type> <interface-id>}] [Neighbor ID]
[detail]
show ip ospf request-list [<neighbor-id>] [{vlan <vlan-id> | <interface-type>
<interface-id>}]
show ip ospf retransmission-list [<neighbor-id>] [{vlan <vlan-id> | <interface-type>
<interface-id>}]
show ip ospf route
show ip ospf virtual-links
show ip ospf {area-range | summary-address}
show ip ospf redundancy
```

This command can be executed in User or in Privileged Mode.

20.30 IP OSPF Key

This command configures operation with IP OSPF packets, carrying specified key.

```
ip ospf key <Key-ID (0-255)> start-accept <DD-MON-YEAR,HH:MM>
ip ospf key <Key-ID (0-255)> stop-accept <DD-MON-YEAR,HH:MM>
ip ospf key <Key-ID (0-255)> start-generate <DD-MON-YEAR,HH:MM>
ip ospf key <Key-ID (0-255)> stop-generate <DD-MON-YEAR,HH:MM>
```

Parameter	Description
start-accept	This command configures the time the router will start accepting packets that have been created with the specified key.
stop-accept	This command configures the time when the router will stop accepting OSPF packets created by using the configured key.
start-generate	This command configures the time when the switch will start generating ospf packets with same key id on the interface.
stop-generate	This command configures the time when the router will stop using configured key for packet generation.
key	Identifies the secret key used to create the message digest appended to the OSPF packet. This value ranges from 0 to 255.
DD-MON-YEAR,HH:MM	Date and Time in 24H format.

This command can be executed in Interface configuration Mode (VLAN interface / Router port).

20.31 Timers SPF

This command configures delay time and hold time between two consecutive SPF calculations.

The no form of the command resets the SPF-delay and SPF-holdtime to its default value.

```
timers spf <spf-delay(0-65535)> <spf-holdtime(0-65535)>
no timers spf
```

Parameter	Description
spf-delay	Configures the interval by which SPF calculation is delayed after a topology change reception. This value ranges from 0 to 65535 seconds.
spf-holdtime	Configures the minimum time between two consecutive SPF calculations. This value ranges from 0 to 65535 seconds.

This command can be executed in OSPF Router Configuration Mode.

20.32 BFD

These commands configure BFD (Bidirectional Forwarding Detection for OSPF) feature.

```
enable bfd
disable bfd
bfd { all-interface | <interface-type> <interface-id> | vlan <vlan-id (1-4094)>}
```

Parameter	Description
enable bfd	This command enables BFD feature in OSPF. This registers OSPF with BFD for neighbor IP path monitoring.
disable bfd	This command disables BFD feature in OSPF. If it is disabled, OSPF will not register with BFD for neighbor IP path monitoring. This is default setting.
bfd interfaces	This command enables BFD monitoring on all or specific OSPF interfaces The no form of the command disables BFD monitoring on all or specific OSPF interfaces

This command can be executed in OSPF Router Configuration Mode.

21 NAT CONFIGURATION

NAT (Network Address Translation) provides a mechanism for privately addressed network to access registered networks, such as the Internet, without requiring a registered subnet address. This eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets.

With NAT, the privately addressed network (designated as inside) continues to use its existing private addresses. These addresses are converted into legal addresses before packets are forwarded onto the registered network (designated as outside). The translation function is compatible with standard routing; the feature is required only on the router connecting the inside network to the outside domain.

NAT feature can be configured either trough CLI or in WEB on Routing → NAT Page.

21.1 IP NAT

This command enables NAT globally.

The no form of the command disables NAT globally.

```
ip nat
no ip nat
```

This command can be executed in Global Configuration Mode.

21.2 IP NAT NAPT

This command enables or disables Network Address Port Translation (NAPT) status on an interface.

WAN interface must be created before the execution of this command for a physical port.

```
ip nat napt {enable|disable}
```

Parameter	Description
enable	Enables NAPT status. If NAPT is enabled, then the same global IP address is overloaded and can be used for many local host by translating the port number.
disable	Disables NAPT status.

This command can be executed in Interface Configuration Mode (Router and VLAN).

21.3 Interface NAT

This command enables or disables NAT status on an interface.

WAN interface must be created before the execution of this command for a physical port.

```
interface nat {enable|disable}
```

Parameter	Description
enable	Enables Interface NAT status.
disable	Disables Interface NAT status

This command can be executed in Interface Configuration Mode (Router and VLAN).

21.4 Static NAT

This command adds a static mapping between local and global address on the specified interface.

The no form of the command deletes the static mapping for the given local IP on the specified interface.

WAN interface must be created before the execution of this command for a physical port.

```
static nat <local ip> <translated local ip>
no static nat <local ip>
```

Parameter	Description
local ip	Configures the actual IP address of the host present in the inside network.
translated local ip	Configures the translated Local IP address. It is the address assigned to the local host by NAT. All the hosts from outside contact the local host through this valid IP Address.

This command can be executed in Interface Configuration Mode (Router and VLAN).

21.5 Port Trigger

This command configures port trigger for outbound and inbound application. Port triggering is an important feature in NAT in which outbound traffic on predetermined ports ('triggering ports') causes inbound traffic on specific incoming ports to be dynamically forwarded to the initiating host.

The no form of the command deletes the configured port trigger for the given application.

```
port trigger <App Name> {tcp|udp|any} <Outbound Port Range> <Inbound Port Range>
no port trigger <App Name>
```

Parameter	Description
App Name	Sets the application name using the port trigger feature.
tcp	Sets the protocol as TCP in the port trigger feature.
udp	Sets the protocol as UDP in the port trigger feature.
any	Sets the protocol other than tcp or udp in the port trigger feature.
Outbound Port Range	Configures the Out-bound port-range through which the inside host initiates the connection.
Inbound Port Range	Configures the Inbound port-range through which the outside host initiates the connection.

This command can be executed in Interface Configuration Mode (Router and VLAN).

21.6 IP NAT Pool

This command adds global address pool.

The no form of the command deletes the global address pool.

WAN interface must be created before the execution of this command for a physical port.

```
ip nat pool <global ip> <mask>
no ip nat pool <global ip>
```

Parameter	Description
global ip	Configures global IP address. It is the IP address network number obtained from the IANA which can be used by NAT for translating the local IP addresses.
mask	Configures the subnet mask. It is the range of global IP Addresses that can be used by the NAT module to translate the local IP Address.

This command can be executed in Interface Configuration Mode (Router and VLAN).

21.7 PORTRANGE

This command configures port forwarding range.

The no form of the command deletes port forwarding range.

WAN interface must be created before the execution of this command for a physical port.

```
portrange <local ip> {tcp|udp|any} <start port no> <end port no>
no portrange <local ip> {tcp|udp|any} <start port no> <end port no>
```

Parameter	Description
local ip	Configures the local IP address.
tcp	Sets the protocol as tcp in the port forwarding range.
udp	Sets the protocol as udp in the port forwarding range.
any	Sets the protocol as any other value other than tcp or udp in the port forwarding range.
start port no	Configures the start Port Number. This value ranges from 1 to 65535.
end port no	Configures the end Port Number. This value ranges from 1 to 65535.

This command can be executed in Interface Configuration Mode (Router and VLAN).

21.8 Static Inside

This command creates a static policy NAT rule binding between the policy NAT identifier and the access-list identifier.

The no form of the command deletes the static policy NAT rule binding between the policy NAT identifier and the access-list identifier.

```
static inside <Policy NAT ID (1-65535)> access-list <string>
no static inside <Policy NAT ID (1-65535)> access-list <string>
```

Parameter	Description
Policy NAT ID	Configures the Policy NAT identifier. It is a unique value, greater than zero, that identifies each NAT Policy binding. This value ranges from 1 to 65535
access-list	Specifies the access-list identifier which creates a static policy NAT rule binding with Policy NAT identifier. The maximum size of string is 36.

This command can be executed in Global Configuration Mode.

21.9 Static Outside

This command adds a static mapping between the traffic (as identified by the access-list identifier) and global address.

```
static outside <Policy NAT ID (1-65535)> <translated local ip>
```

Parameter	Description
Policy NAT ID	Configures the Policy NAT identifier. It is a unique value, greater than zero, that identifies each NAT Policy binding. This value ranges from 1 to 65535
translated local ip	Configures the translated Local IP. It is the address assigned to the local host by NAT. All the hosts from outside will contact the local host through this valid IP Address

This command can be executed in Global Configuration Mode.

21.10 NAT Inside

This command creates a dynamic policy NAT rule binding between the policy NAT identifier and the access-list identifier.

The no form of the command deletes the dynamic policy NAT rule binding between the policy NAT identifier and the access-list identifier

```
nat inside <Policy NAT ID (1-65535)> access-list <string>
no nat inside <Policy NAT ID (1-65535)> access-list <string>
```

Parameter	Description
Policy NAT ID	Configures the Policy NAT identifier. It is a unique value, greater than zero, that identifies each NAT Policy binding. This value ranges from 1 to 65535
access-list	Specifies the access-list identifier which creates a dynamic policy NAT rule binding with Policy NAT identifier.The maximum size of string is 36.

This command can be executed in Global Configuration Mode.

21.11 NAT Outside

This command creates a dynamic policy NAT rule binding between the policy NAT identifier and the access-list identifier.

The no form of the command deletes the dynamic policy NAT rule binding between the policy NAT identifier and the access-list identifier.

```
nat inside <Policy NAT ID (1-65535)> access-list <string>
no nat inside <Policy NAT ID (1-65535)> access-list <string>
```

Parameter	Description
Policy NAT ID	Configures the Policy NAT identifier. It is a unique value, greater than zero, that identifies each NAT Policy binding. This value ranges from 1 to 65535
access-list	Specifies the access-list identifier which creates a dynamic policy NAT rule binding with Policy NAT identifier.The maximum size of string is 36.

This command can be executed in Global Configuration Mode.

21.12 IP NAT Timeout

This command sets the NAT timeout value for the TCP, UDP or Idle configuration.

The no form of this command resets the NAT time out for the TCP, UDP or Idle configuration to its default value.

```
ip nat {idle timeout <seconds (60-86400)> | {tcp | udp } timeout <seconds (300-86400)>}
no ip nat {idle | tcp | udp } timeout
```

Parameter	Description
idle timeout	Sets the timeout value for NAT idle configuration. The idle time out value is the amount of time (in seconds) until which a connection can stay idle, and after which the connection will be terminated. This value ranges from 60 to 86400 seconds. Default: 60 seconds.
tcp timeout	Sets the timeout value for NAT TCP configuration. The tcp timeout is the amount of time (in seconds) for which the TCP session entry can be present in the NAT session table without being used or referred, before being removed from the NAT session table. This value ranges from 300 to 86400 seconds. Default: 3600 seconds.
udp timeout	Sets the timeout value for NAT UDP configuration. The udp timeout is the amount of time (in seconds) for which the UDP session entry can be present in the NAT session table without being used or referred, before being removed from the NAT session table. This value ranges from 300 to 86400 seconds. Default: 300 seconds

This command can be executed in Global Configuration Mode.

21.13 Show NAT

This command displays various NAT-related parameters and statuses.

```
show nat config
show ip nat interface
show ip nat { global | static | translations | policy}
```

Parameter	Description
config	This command displays NAT configuration.
interface	This command displays NAT interface configuration.
ip nat	This command displays various NAT tables: • global - Displays Global IP NAT configurations • static - Displays Static IP NAT configurations • translations - Displays NAT Translations • policy - Displays NAT Policy configurations

This command can be executed in User or Privileged Mode.

22 VPN

A virtual private network (VPN) is a private communications network used by companies or organizations, to communicate confidentially over a public network. VPN traffic is carried over a public networking infrastructure (Example: Internet).VPN connections are more cost-effective than dedicated private lines.

The GigaFlex realisation of VPN supports IPSec and IKE.

VPN can be configured either through CLI or in WEB on Network Security Page.

The IPSec license should be previously activated for this feature.

22.1 Set VPN

This command enables or disables the VPN module for encryption and decryption of the flows and administratively IP Security processing.

```
set vpn {enable | disable}
```

Parameter	Description
enable	Enables the VPN module for encryption and decryption of the flows and administratively IP Security processing.
disable	Disables the VPN module for encryption and decryption of the flows and administratively IP Security processing.

This command can be executed in Global Configuration Mode.

22.2 Crypto Map

This command creates a new crypto map which defines the VPN policy to be negotiated for Security Association creation and brings up the policy, key, transform-set and access-list. The Crypto-maps can have many line numbers and they can be defined by their own names which should be used to apply the crypto-map to the interface.

The no form of the command deletes the crypto map.

```
crypto map <policy-name>
no crypto map {<map-name> | all}
```

Parameter	Description
policy-name / map-name	Configures the name of the crypto map. The size of the string ranges between 0 and 50.
all	Deletes all the policies

This command can be executed in Global Configuration Mode.

22.3 Crypto Key Mode

This command specifies the type of VPN used and configures the type of the mode in which the crypto-map entry is performed.

```
crypto key mode {ipsec-manual | preshared-key | cert | xauth | ravpn-preshared-key | ra-cert |
xauth-cert }
```

Parameter	Description
ipsec-manual	Estabishes the IPSEC manual security associations (SAs) for protecting the traffic specified by this crypto map entry.

preshared-key	Configures the Preshared Key which is the authentication method used for ike phase -1 negotiation.
cert	Configures the certificate information about the security router.
xauth	Configures the VPN crypto key mode as extended authentication.
ravpn-preshared-key	Configures the authentication mode specific to RA VPN policy. In this mode, authentication is done with Preshared key only (without user authentication).
ra-cert	Configures the remote access certificate. If this certificate is selected, the policy uses a remote access vpn policy using authentication as RSA method.
xauth-cert	Configures Extended authentication certificate. If xauth-certificate is selected , the policy is a remote access vpn policy with extented authentication using RSA authentication method.

This command can be executed in Crypto Map Configuration Mode.

22.4 Crypto Map Access-List

This command specifies the source and destination IP address to which the policy is applied with the type of traffic and action to be taken. This command configures the Proto index value which uniquely identifies the protocol for which this Selector Table entry exists. In case of no specific protocol any can be used.

```
access-list {permit|deny|apply} {any|tcp|udp|icmpv4|ahproto|espproto} source <ip-address>
<subnet-mask> destination <ip-addrress> <subnet-mask> [srcport (0-65535)] [destport (0-65535)]
```

Parameter	Description
permit	Permits the Access list for the source and destination IP address. The list contains: • any – Permits the Access list for the source and destination IP address for any protocol • tcp - Permits the Access list for the source and destination IP address for TCP protocol • udp - Permits the Access list for the source and destination IP address for UDP protocol • icmpv4 - Permits the Access list for the source and destination IP address for ICMPv4 protocol • ahproto - Permits the Access list for the source and destination IP address for AH protocol • espproto - Permits the Access list for the source and destination IP address for ESP protocol
deny	Denies the Access list for the source and destination IP address. The list contains; • any – Denies the Access list for the source and destination IP address for any protocol • tcp - Denies the Access list for the source and destination IP address for TCP protocol • udp - Denies the Access list for the source and destination IP address for UDP protocol

	• icmpv4 - Denies the Access list for the source and destination IP address for ICMPv4 protocol • ahproto - Denies the Access list for the source and destination IP address for AH protocol • espproto - Denies the Access list for the source and destination IP address for ESP protocol
apply	Applies the Access list for the source and destination IP address. The list contains; • any – Applies the Access list for the source and destination IP address for any protocol • tcp - Applies the Access list for the source and destination IP address for TCP protocol • udp - Applies the Access list for the source and destination IP address for UDP protocol • icmpv4 - Applies the Access list for the source and destination IP address for ICMPv4 protocol • ahproto - Applies the Access list for the source and destination IP address for AH protocol • espproto - Applies the Access list for the source and destination IP address for ESP protocol
source <ip-address>	Configures the Source IP Address
source <subnet-mask>	Configures the Source IP Subnet Mask
destination <ip-addrress>	Configures the Destination IP Address
destination <subnet-mask>	Configures the Destination IP Subnet Mask
srcport (0-65535)	Configures the Source port. This value ranges from 0 to 65535.
destport (0-65535)	Configures the Destination port This value ranges from 0 to 65535.

This command can be executed in Crypto Map Configuration Mode.

22.5 Crypto Map - Interface

This command applies the crypto policy to the specified interface. A crypto map set must be assigned to an interface before that interface can provide IPSec services, only one crypto map set can be assigned to an interface.

The no form of the command disables the policy applied to the specific interface.

```
crypto map <policy name>
no crypto map <policy-name>
```

Parameter	Description
policy-name / map-name	Configures the name of the crypto map. The size of the string ranges between 0 and 50.

This command can be executed in Interface Configuration Mode.

22.6 RA-VPN Username

This command configures usernames and password to identify remote access users to the device when acting as a RAVPN Server.

The no form of the command deletes the existing users from accessing Remote Access VPN.

```
ra-vpn username <username> password <password>
no ra-vpn username <username>
```

Parameter	Description
username	Configures an user name which is the index for accessing the Remote Users table. The value is of Alphanumeric characters of length 1 to 32.
password	Configures an password for remote user where the value is of Alphanumeric characters of length 1 to 32. The length of the password must be greater than or equal to 4 characters and less than or equal to 31 characters.

This command can be executed in Global Configuration Mode.

22.7 IP RA-VPN Pool

This command configures an IP address pool for assigning IP addresses for remote users using local address pool. The Start and end IP address should be specified for each pool.

The no form of the command deletes the IP address pool for remote users.

```
ip ra-vpn pool <poolname> <start_ip> - <end_ip>
no ip ra-vpn pool <poolname>
```

Parameter	Description
poolname	Configures the pool name which is the index for accessing the Remote Access Address Pool table The value of the IP Address pool name which is a string of length 1 to 32.
start_ip - end_ip	Configures the starting and ending ip address of the remote users.The start and end IP must belong to the same subnet.

This command can be executed in Global Configuration Mode.

22.8 VPN Remote Identify

This command configures the remote identity information and its pre-shared key. The remote identity and the pre-shared keys are globally available to all the VPN tunnels and can be mapped whenever required. One identity can be mapped to multiple tunnels.

The no form of the command deletes the remote id and its pre-shared key mappings.

```
vpn remote identity {ipv4 | email | fqdn | dn | keyId | ipv6} <id-value> { psk | cert }
<preshared-key> /<key-id>
no vpn remote identity {ipv4 | email | fqdn | dn | keyId | ipv6} <id-value>
```

Parameter	Description
ipv4	Configures the IPv4 address for which the remote identity information is configured.
email	Configures the E-mail address.
fqdn	Configures the fully qualified domain name.
dn	Configures the Domain name.
keyId	Configures the string which is used to uniquely identify the peer.
ipv6	Configures the IPv6 address for which the remote identity information.
id-value	Deletes the remote identifier.

psk	Configures the pre-shared key.
cert	Configures the certificate information about the security router.
preshared-key / key-id	Configures the pre-shared key with the gateway. The PSK is used by the gateway to authenticate the phase-IIKE transactions with this user.

This command can be executed in Global Configuration Mode.

22.9 VPN Gen Key

This command creates a new RSA or DSA key pair. The keys are generated in pairs—one public key and one private key. If your router already has RSA/ DSA keys when issuing this command, you will be warned and prompted to replace the existing keys with new keys.

```
vpn gen key <keyname> {rsa| dsa } nbits {512|1024|2048|4096}
```

Parameter	Description
keyname	Specifies RSA or DSA key name.
rsa	Configures the Ron Rivest, Adi Shamir and Len Adleman Algorithm to generate the key.
dsa	Configures Digital Signature Algorithms to generate the key.
nbits {512|1024|2048|4096}	Configures the key size to be n bit. The options are given below • 512 – Configures the key size as 512 • 1024 – Configures the key size as 1024 • 2048 – Configures the key size as 2048 • 4096 – Configures the key size as 4096

This command can be executed in Global Configuration Mode.

22.10 VPN Import

This command imports a key pair from the specified file, into the database. This configuration is used to import an RSA/ DSA key pair, if the user already has the RSA key pair and the corresponding certificate.

The no form of the command deletes specific node if key-name is specified else deletes all entries.

```
vpn import {rsa|dsa} key <keyname> file <filename>
no vpn {rsa|dsa} key {index <keyname> | all}
```

Parameter	Description
rsa	Configures the Ron Rivest, Adi Shamir and Len Adleman Algorithm to import a key pair from the specified file into the database
dsa	Configures Digital Signature Algorithms to import a key pair from the specified file into the database.
key / index	Configures the RSA key name for the imported RSA key.
file	Configures the File name in which the RSA keys are imported
all	Deletes all entries of the VPN RSA Key

This command can be executed in Global Configuration Mode.

22.11 VPN Import

This command imports the certificate from file.

The no form of the command deletes specific node if key-name is specified else deletes all entries.

```
vpn import cert file <filename> encode-type {PEM|DER} key <keyid>
no vpn cert {index <keyname> | all}
vpn import peer-cert <PeerCertId> file <filename> encode-type {PEM|DER} [trusted]
no vpn peer-cert {index <peercertindex> | dynamic | all}
vpn import ca-cert <CaCertId> file <filename> encode-type {PEM|DER}
no vpn ca-cert {index <CaCertId> | all}
```

Parameter	Description
cert file	This command encodes the files and imports the certificate from file, which contains information about the security router. The no form of the command deletes specific node if keyname is specified else deletes all entries.
peer-cert	This command imports peer certificate from a given file which contains information about the peer security router. The no command deletes specific node(s) if certificate index or dynamic is specified else deletes all entries.
ca-cert	This command imports ca certificate from a given file. The no form of the command deletes specific node if CA index is specified else deletes all entries.
file	Confiures the File name for import.
encode-type	Configures the type of encoding used to import the file. • PEM – Configures the type for encoding as Privacy Enhanced Mail Encoding • DER - Configures the type of encoding as Distinguished Encoding Rules Encoding
key	Configures the Key identifier value.
index	Deletes the RSA key name for the imported RSA key.
all	Deletes all entries.
PeerCertId / index	Configures the Peer certificate identifier to import a file.
trusted	Configures Trusted peer certificate. If this option is given peer certificate is trusted , otherwise it is an untrusted certificate.
dynamic	Deletes the specific node for the specified dynamic.
CaCertId / index	Configures the Certificate Authority identifier value.

This command can be executed in Global Configuration Mode.

22.12 VPN Save Certs

This command saves my certificates , trusted peer certificates, CA certificates and RSA keys to the file system.

```
vpn save certs
```

This command can be executed in Global Configuration Mode.

22.13 VPN Remote-Access

This command configures the security router as remote access VPN client or server.

```
vpn remote-access  {server | client}
```

Parameter	Description
server	Sets security router as remote access vpn server.
client	Sets security router as remote access vpn client.

This command can be executed in Global Configuration Mode.

22.14 IKE Trigger

This command triggers IKE negotiation for remote access client with specified peer ip address.

```
ike trigger <ipaddress>
```

This command can be executed in Global Configuration Mode.

22.15 SET IKE Version

This command specifies the IKE version to be used for a particular policy and for key negotiation.

```
set ike version {v1 | v2}
```

Parameter	Description
v1	Configures the IKE Version as 1.
v2	Configures the IKE Version as 2.

This command can be executed in Crypto Map Configuration Mode.

22.16 SET Peer

This command sets the destination ip address in the packet during authentication and encryption of outbound datagrams.

```
set peer <peer-ip>
```

Parameter	Description
peer-ip	Configures the peer destination ip address

This command can be executed in Crypto Map Configuration Mode.

22.17 Crypto IPSec Mode

This command sets the IPSEC mode.

```
crypto ipsec mode {tunnel | transport}
```

Parameter	Description
tunnel	Sets the mode as tunnel. When this mode is configured, IPSec encrypts the IP header and the payload tunnel mode provides the protection of an entire IP packet by treating it as an AH or ESP payload. With tunnel mode, an entire IP packet is encapsulated with an AH or ESP header and an additional IP header. The IP addresses of the outer IP header are the tunnel endpoints, and the IP addresses of the encapsulated IP header are the ultimate source and destination addresses.

transport	Sets the transport mode which is used for end-to-end communications. When this mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header.

This command can be executed in Crypto Configuration Map Mode.

22.18 Set Session Key

This command specifies the mode of VPN along with the authentication and encryption algorithm with inbound and outbound SPI.

```
set session-key {[authenticator {ah | esp} {hmac-md5 | hmac-sha1 | xcbc-mac | hmac-sha-256
|hmac-sha-384 | hmac-sha-512 } <auth-key>] [esp {des cipher <key> | triple-des cipher <key1>
<key2> <key3> | {aes | aes-192 | aes-256} cipher <key>}]} outbound <spi (256-2147483647)>
inbound <spi(256-2147483647)> [anti-replay]
```

Parameter	Description
authenticator	Configures the authenticator. The options are: • ah - Authenticator with Authentication Header • esp - Authenticator with Encapsulating Security Payload
hmac-md5	Sets the key used for authentication when the algorithm configured as hmac-md5. For hmac-md5 the fixed key size must be 16 bytes.
hmac-sha1	Sets the key used for authentication when the algorithm configured as hmac-sha1. For hmac-sha1 the fixed key size must be 20 bytes.
xcbc-mac	Sets the key used for authentication when the algorithm configured as xcbc-mac. For xcbc-mac the fixed key size must be 16 bytes.
hmac-sha-256	Sets the key used for authentication when the algorithm configured as hmac-sha-256. For hmac-sha-256 the fixed key size must be 32 bytes.
hmac-sha-384	Sets the key used for authentication when the algorithm configured as hmac-sha-384. For hmac-sha-384 the fixed key size must be 48 bytes.
hmac-sha-512	Sets the key used for authentication when the algorithm configured as hmac-sha-512. For hmac-sha-512 the fixed key size must be 64 bytes.
des cipher	Configures Data Encryption Standard (DES) algorithm which is used for encryption of the Encapsulating Security Payload. • <key> - Encrypts and decrypts when the algorithm configured is descbc, 3descbc or aes128, aes192 or aes256. The size of the string ranges between 0 and 256 bytes.
triple-des cipher	Configures Triple Data Encryption Standard algorithm which is used for encryption of Encapsulating Security Payload The value of all 3 keys should be unique.
aes-128	Sets Advanced Encryption Standard (AES) algorithm with a 128-bit key for encryption of the Encapsulating Security Payload.
aes-192	Sets Advanced Encryption Standard with a 192-bit key for encryption of the Encapsulating Security Payload
aes-256	Sets Advanced Encryption Standarwith a 256-bit key for encryption of the Encapsulating Security Payload.
outbound	Configures the outbound Security Parameter Index. This value ranges from 256 to 2147483647.

inbound	Configures the inbound Security Parameter Index. This value ranges from 256 to 2147483647.
anti-replay	Configures ani-replay for activating the anti replay functionality of the security protocols.

This command can be executed in Crypto Map Configuration Mode.

22.19 ISAKMP Peer Identity

This command associates the remote identity with the policy to use in IKE negotiations and defines the ISAKMP identity used by the router when participating in the Internet Key Exchange (IKE) protocol. An ISAKMP identity is set whenever you specify pre-shared keys or RSA signature authentication.

```
isakmp peer identity {ipv4|email|fqdn|dn|keyId|ipv6} <id-value>
```

Parameter	Description
ipv4	Sets the ISAKMP identity to the IP4 address of the interface that is used to communicate to the remote peer during IKE negotiations.
email	Sets the type as E-mail address for remote peer.
fqdn	Sets the type as Fully Qualified Domain Name for remote peer.
dn	Sets the type as domain for remote peer.
keyId	Sets the type as Key identifier for the remote peer.
ipv6	Sets the ISAKMP identity to the IP6 address of the interface that is used to communicate to the remote peer during IKE negotiations.
id-value	Configures the peer identity value corresponding to the selected Identity.

This command can be executed in Crypto Map Configuration Mode.

22.20 ISAKMP Local Identity

This command configures the local identity type and its value to be used in IKE Phase 1. It can be IP address, email, FDQN or key id.

```
isakmp local identity {ipv4|email|fqdn|dn|keyId|ipv6} <id-value>
```

Parameter	Description
ipv4	Sets the ISAKMP identity to the IP4 address of the interface that is used to communicate to the local identity during IKE negotiations.
email	Sets the type as E-mail address for local identity.
fqdn	Sets the type as Fully Qualified Domain Name for local identity.
dn	Sets the type as domain for local identity.
keyId	Sets the type as Key identifier for the local identity.
ipv6	Sets the ISAKMP identity to the IP6 address of the interface that is used to communicate to the local identity during IKE negotiations.
id-value	Configures the local identity value corresponding to the selected identity.

This command can be executed in Crypto Map Configuration Mode.

22.21 ISAKMP Policy Encryption

This command specifies IKE Phase I Proposal with encryption and authentication algorithm, mode of transaction and lifetime as parameters and invokes the Internet Security Association Key Management Protocol (ISAKMP) policy configuration. Multiple IKE policies can be configured on each peer participating in IPsec.

```
isakmp policy encryption {des | triple-des | aes | aes-192 | aes-256} hash {md5 | sha1 | sha256
| sha384 | sha512} dh {group1|group2|group5|group14} [exch {main|aggressive}] lifetime
{secs|mins|hrs} <lifetime>
```

Parameter	Description
des	Configures Data Encryption Standard (DES) algorithm which is used for encryption of the Encapsulating Security Payload.
triple-des	Configures Triple Data Encryption Standard algorithm which is used for encryption.
aes	Configures Advanced Encryption Standard (AES) algorithm for encryption.
aes-192	Configures Advanced Encryption Standard with a 192-bit key for encryption.
aes-256	Configures Advanced Encryption Standarwith a 256-bit key for encryption.
hash	Configures Hash algorithm related configurations. • md5 - Specifies to use Message Digest 5 (MD5) as the hash algorithm and produces 128-bit hash values. • sha1- Specifies to use Secure Hash Algorithm (SHA) as the hash algorithm and produces 160-bit hash values. • sha256- Specifies to use Secure Hash Algorithm (SHA) as the hash algorithm and produces 256-bit hash values. • sha384- Specifies to use Secure Hash Algorithm (SHA) as the hash algorithm and produces 384-bit hash values. • sha512- Specifies to use Secure Hash Algorithm (SHA) as the hash algorithm and produces 512-bit hash values.
dh	Configures the typeIKE group, the options are • group1 - Configures the type IKE group1. Specifies to use 768-bit Diffie-Hellman Group 1 cryptography. • group2 - Configures the type IKE group2, Specifies to use 1024-bit Diffie-Hellman Group 2 cryptography. • group5 - Configures the type IKE group5. Specifies to use 1536-bit Diffie-Hellman Group 5 cryptography. • group14 - Configures the type IKE group14. Specifies to use 2048-bit Diffie-Hellman Group 14 cryptography.
main	Specifies the IKE Phase 1 mode, as main.
aggressive	Specifies the IKE Phase 1 mode, as aggressive.
lifetime	Configures the IPSec SA life time type. The SA is re-negotiated after the time limit elapses. The options are: • sec- Configures the IPsec SA life time in secs • min- Configures the IPsec SA life time in min • hrs- Configures the IPsec SA life time in hrs

lifetime	Configures the IPSec SA life time type. This value ranges from 300 to 86400 seconds.

This command can be executed in Crypto Map Configuration Mode.

22.22 Crypto Map IPSec

This command specifies the IKE Phase II Proposal with encryption and authentication algorithm, mode of transaction and lifetime as parameters.

```
crypto map ipsec {[encryption esp {null | des | triple-des | aes |aes-192 | aes-256 | aes-ctr |
aes-ctr-192 | aes-ctr-256}] [authentication {esp | ah} {md5 | sha1 |xcbc-mac| hmac-sha-256
|hmac-sha-384 | hmac-sha-512  }]} [pfs {group1 | group2 | group5| group14}] [lifetime {secs |
mins | hrs | kb} <lifetime>]
```

Parameter	Description
encryption esp	Configures the encryption algorithm. The Options are: • null-Configures null algorithm • des -Configures Data Encryption standard algorithm • triple-des-Configures triple Data Encryption Standard algorithm • aes-Configures advanced encryption standard with 128-bit key for encryption • aes-192-Configures advanced encryption standard with 192-bit key for encryption • aes-256-Configures advanced encryption standard with 256-bit key for encryption • aes-ctr - Configures advanced encryption standard counter mode with 128-bit key for encryption. • aes-ctr-192- Configures advanced encryption standard counter mode with 192-bit key for encryption • aes-ctr-256--Configures advanced encryption standard counter mode with 256-bit key for encryption

authentication	Configures the authentication algorithm. The options to configure the security protocol header are:
	• ah - Configures authentication header algorithm related information.
	• esp - Configures Encapsulating security payload algorithm related information. The options are:
	  ○ md5 - Specifies to use Message Digest 5 (MD5) as the hash algorithm and produces 128-bit hash values.
	  ○ sha1- Specifies to use Secure Hash Algorithm (SHA) as the hash algorithm and produces 160-bit hash values.
	  ○ xcbc-mac – Sets the key used for authentication when the algorithm configured as xcbc-mac. For xcbc-mac the fixed key size must be 16 bytes.
	  ○ hmac-sha-256- Sets the key used for authentication when the algorithm configured as hmac-sha-256.For hmac-sha-256 the fixed key size must be 32 bytes

	○ hmac-sha-384 - Sets the key used for authentication when the algorithm configured as hmac-sha-384.For hmac-sha-384 the fixed key size must be 48 bytes ○ hmac-sha-512 - Sets the key used for authentication when the algorithm configured as hmac-sha-512. For hmac-sha-512 the fixed key size must be 64 bytes.
pfs	Configures perfect forward secrecy: • group1 - Configures the type IKE group1. Specifies to use 768-bit Diffie-Hellman Group 1 cryptography. • group2 - Configures the type IKE group2, Specifies to use 1024-bit Diffie-Hellman Group 2 cryptography. • group5 - Configures the type IKE group5. Specifies to use 1536-bit Diffie-Hellman Group 5 cryptography. • group14 - Configures the type IKE group14. Specifies to use 2048-bit Diffie-Hellman Group 14 cryptography.
main	Specifies the IKE Phase 1 mode, as main.
aggressive	Specifies the IKE Phase 1 mode, as aggressive.
lifetime	Configures the IPSec SA life time type. The SA is re-negotiated after the time limit elapses. The options are: • sec- Configures the IPsec SA life time in secs • min- Configures the IPsec SA life time in min • hrs- Configures the IPsec SA life time in hrs • kb - Configures the life time in Kilobytes. This value ranges from 100 to 10000000 KB.

This command can be executed in Crypto Map Configuration Mode.

22.23 IPv6 RA-VPN Pool

This command configures IPv6 address pool for the remote users connected via VPN tunnel. The IP addresses are allocated to the remote users based on the local address pool.

```
ipv6 ra-vpn pool <poolname> <start_ipv6> - <end_ipv6> <prefixlen>
no ip ra-vpn pool <poolname>
```

Parameter	Description
poolname	Configures the name for the local address pool. This name acts as an index for accessing the particular entry from the local address pool table. The maximum length of this name should be 32 characters.
start_ipv6	Configures the starting IPv6 address of the pool for remote users. This value is used along with end IPv6 address to define the range of pool. The IPv6 address allocated to the remote users should be within this range.
end_ipv6	Configures the last IPv6 address of the pool for remote users. This value is used along with start IPv6 address to define the range of pool. The IPv6 address allocated to the remote users should be within this range.
prefixlen	Configures the prefix length for the local address pool. This length is applied to the start and end IPv6 addresses for generating range of IPv6 addresses. This value ranges from 0 to 128.

This command can be executed in Global Configuration Mode.

22.24 IKE IPv6 Trigger

This command triggers IKE negotiation with specified peers. The router receives all IKE policies from remote peers. The router then scans its own list of IKE policies to check whether a match exists, starting from the highest priority. If it finds a match, the respective policy is successfully negotiated.

```
ike ipv6 trigger <IPv6 address>
```

This command can be executed in Global Configuration Mode.

22.25 Set IPv6 Peer

This command configures the destination address in the packet during authentication and encryption of outbound datagrams.

```
set ipv6 peer <peer-ipv6 address>
```

This command can be executed in Global Configuration Mode.

22.26 Crypto Map Access-List IPv6

This command configures the source and destination IPv6 address to which the IKE policy is to be applied along with the type of traffic and action to be taken.

```
access-list ipv6 { permit | deny | apply}  {any | tcp | udp | icmpv4 | ahproto | espproto}
source <ipv6-address> <prefixlen> destination<ipv6-addrress> <prefixlen> [srcport (0-65535)]
[destport (0-65535)]
```

Parameter	Description
permit	Permits the Access list for the source and destination IPv6 address. The list contains: • any – Permits the Access list for the source and destination IP address for any protocol • tcp - Permits the Access list for the source and destination IP address for TCP protocol • udp - Permits the Access list for the source and destination IP address for UDP protocol • icmpv4 - Permits the Access list for the source and destination IP address for ICMPv4 protocol • ahproto - Permits the Access list for the source and destination IP address for AH protocol • espproto - Permits the Access list for the source and destination IP address for ESP protocol
deny	Denies the Access list for the source and destination IP address. The list contains; • any – Denies the Access list for the source and destination IP address for any protocol • tcp - Denies the Access list for the source and destination IP address for TCP protocol • udp - Denies the Access list for the source and destination IP address for UDP protocol

	• icmpv4 - Denies the Access list for the source and destination IP address for ICMPv4 protocol • ahproto - Denies the Access list for the source and destination IP address for AH protocol • espproto - Denies the Access list for the source and destination IP address for ESP protocol
apply	Applies the Access list for the source and destination IP address. The list contains; • any – Applies the Access list for the source and destination IP address for any protocol • tcp - Applies the Access list for the source and destination IP address for TCP protocol • udp - Applies the Access list for the source and destination IP address for UDP protocol • icmpv4 - Applies the Access list for the source and destination IP address for ICMPv4 protocol • ahproto - Applies the Access list for the source and destination IP address for AH protocol • espproto - Applies the Access list for the source and destination IP address for ESP protocol
source <ipv6-address>	Configures the Source IPv6 Address
source <prefixlen>	Configures the prefix length for the outbound traffic. This length is applied to the source IPv6 address for generating range of source IPv6 addresses to be used for the VPN policy. This value ranges from 0 to 128.
destination <ipv6-address>	Configures the destination IPv6 address of the outbound traffic. This IPv6 address is used to identify the destination network for the VPN policy. This IP route should have been already configured for the specified destination address.
destination <prefix-len>	Configures the prefix length for the outbound traffic. This length is applied to the destination IPv6 address for generating range of destination IPv6 addresses to be used for the VPN policy. This value ranges from 0 to 128.
srcport (0-65535)	Configures the Source port. This value ranges from 0 to 65535.
destport (0-65535)	Configures the Destination port This value ranges from 0 to 65535.

This command can be executed in Crypto Map Configuration Mode.

22.27 Crypto Key Encrypt

This command configures the type of algorithm to be used for encryption.

```
crypto key encrypt {rsa | dsa}
```

Parameter	Description
rsa	Sets the Ron Rivest, Adi Shamir and Len Adleman Algorithm which is used for encryption.
dsa	Sets the Digital Signature Algorithms which is used for encryption.

This command can be executed in Crypto Map Configuration Mode.

22.28 Crypto Key Decrypt

This command configures the type of algorithm to be used for decryption.

```
crypto key decrypt {rsa | dsa}
```

Parameter	Description
rsa	Sets the Ron Rivest, Adi Shamir and Len Adleman Algorithm which is used for decryption.
dsa	Sets the Digital Signature Algorithms which is used for decryption.

This command can be executed in Crypto Map Configuration Mode.

22.29 Show RA-VPN

his command displays information configured to do remote access

```
show ra-vpn users
show ra-vpn address-pool
```

Parameter	Description
users	This command displays user information configured to do remote access.
address-pool	This command displays IP address pool assigned for remote users.

This command can be executed in User or in Privileged Mode.

22.30 Show VPN

This command displays various VPN-related information.

```
show vpn config
show crypto map [<policy name>]
show vpn global statistics
show vpn ike statistics
show vpn {rsa|dsa} keys
show vpn certs [index <keyid>]
show vpn peer-certs [index <PeerCertId> | dynamic]
show vpn ca-certs [index <CaCertId>]
show vpn map-cert
```

Parameter	Description
config	This command displays the global VPN settings.
crypto map	This command displays the crypto policy parameters of the specified interface.
global statistics	This command displays the In, Out, Secured, Dropped Packet in the VPN module.
ike statistics	This command displays the IKE and IPSec Security Associations (SA) statistics.
keys	This command displays RSA or DSA key pairs generated in the system.
certs	This command displays vpn certificates.
peer-certs	This command displays vpn peer certificates.
ca-certs	This command displays vpn CA certificates.
map-cert	This command displays certificate mapping with the peer.

This command can be executed in User or in Privileged Mode.