PDS-204GCO™ Command Line Interface User Guide

Introduction

PDS-204GCO™ is a next-generation outdoor Power over Ethernet (PoE) switch for smart cities. It allows Wi-Fi® access points, security network cameras, and many other IoT devices to receive power and data over standard Ethernet cables, leaving network infrastructure completely unaltered.

This user guide describes the Command-Line Interface (CLI) of the PDS-204GCO network switch.

Table of Contents

1. Command Line Interface

CLI is used for configuring, monitoring, and maintaining the PDS-204GCO switch over CLI, Telnet, and SSH.

Important:

- It is strongly recommended to use the Web interface to simplify user configuration and reduce configuration mismatch.
- CLI interface might contain more configuration commands vs. those affected as a result or user configuration changes over the web. This manual covers only those commands that are affected when you change unit configuration over the Web interface.

All commands entered in CLI are followed by values, parameters, or both. Parameters might be mandatory values, optional values, choices, or a combination.

- **<parameter>**: The < > angle brackets indicate that a mandatory parameter is to be entered in place of the brackets and text inside them.
- **[parameter]**: The [ ] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.
- **choice1 | choice2**: The | indicates that only one of the parameters should be entered.
- **{ }**: The { } curly braces indicate that a parameter must be chosen from the list of choices.

Values might be in a form of six hexadecimal numbers separated by the following:

- Colons (MAC address). For example, 00:06:29:32:81:40.
- Dotted-decimal notation (Area IDs). For example, 0.0.0.1.
- Slot/port number. For example, 1/1 or logical slot/port (applicable in case of a link-aggregation).

1.1 Completing Partial Command

Enter the first few letters of the command, and then press **Tab**. The command line parser completes the command if the entered string is unique to the command. Another option is to type the first few letters followed by (?). This shows all the commands that start with the letters you have already typed.

1.2 Command History

Use the **Up/Down** arrows keys to scroll between the commands. To display the entire history, use the `show history` command.

2. General Maintenance Commands

The following sections describe the General Maintenance commands.

2.1 configure terminal

Description
Start unit configuration. Terminal display switches from `#` to `(config)#`.

```
configure terminal
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	EXEC	
Usage	Enter configuration mode when starting unit configuration.	
Example	`# configure terminal`[1]	

Note:
1. You can also use the shortcut `# conf t`.

2.2 interface

Description
Start interface (port) configuration. Terminal display switches from `(config)#` to `(config-if)# interface <port_type> [ <port_type_list> ]`.

Note: You can configure same parameter for multiple interfaces by using syntax as 1/1–4 (configure same value for ports 1–4), as described in the command example.

	Argument	Description
Parameter	`<port_type>`	Port type Gigabit Ethernet 2.5 Gigabit Ethernet VLAN
	`[ <port_type_list> ]`	List of Port ID. For example, 1/1, 2-4 1/1-4 1/1, 2, 4.
Default	NA	
Mode	Global Configuration mode	
Usage	Enter the Interface Configuration mode to start configuring the port parameters.	

Example	1. Enter the configuration mode for ports 1 and 4.
	`(config)# interface GigabitEthernet 1/1, 4`
	`(config-if)#`
	2. Enter the configuration mode for ports 1 through 4.
	`(config)# interface GigabitEthernet 1/1-4`
	`(config-if)#`	

2.3 exit

Description
Go up one level in the configuration process. Logout from terminal/telnet/SSH session in case user was at top level.

```
exit
```

	Argument	Description
Parameter	—	NA
Default	NA	
Mode	Exit from current mode	
Usage	Use this command when you end in-depth configuration and must go up one level or to log out of the serial interface.	

Example	1. `(config)# exit`
	`#`
	2. `(config-if)# exit`
	`(config)#`	

2.4 end

Description
Use this command to end any in-depth configuration mode and return to the EXEC mode.

```
end
```

	Argument	Description
Parameter	—	NA
Default	NA	
Mode	Return to the EXEC mode	
Usage	When you must end in-depth configuration and return to the EXEC mode.	
Example	1. `(config-if)# end` `#` 2. `(config)# end`	

2.5 dir

Description
This command shows all optional configuration files stored inside the unit.

```
dir
```

	Argument	Description
Parameter	—	—
Default	NA	
Mode	EXEC	

.....continued		
	Argument	**Description**
Usage	Use this command to view all configuration files stored in the flash.	
Example	`# dir`	

2.6 show version

Description
Use this command to display unit software and hardware information.

```
show version
```

	Argument	**Description**
Parameter	—	—
Default	NA	
Mode	EXEC	
Usage	Use this command to display unit information.	
Example	`cm`	

3. Configuration Commands

The following sections describe the Configuration commands.

3.1 System Configuration commands

The following sections describe the configure system information, IP, SNMP, NTP, and Time and Log parameters.

3.1.1 System Information Configuration

Description

Use this command to specify SNMP MIB-II contact person, system name, and system location.

```
snmp-server contact <v_line255>
```

```
host <conf_name>
```

```
snmp-server location <v_line255>
```

	Argument	Description
Parameter	<v_line255>	String length is 0–255 and valid ASCII characters range is 32–126.
	<conf_name>	Administratively assigned name for this system. By convention, this is a fully qualified domain name. String length is 0–255 and spaces are not permitted.
Default	NA	
Mode	Global Configuration mode	
Usage	Specify system contact, name, and location. Use the no version of the command to delete it.	
Example	Set system contact as **testcontact**, name as **microchip** and location as **server room**: # configure terminal (config)# snmp-server contact testcontact (config)# host microchip microchip(config)# snmp-server location server room	

3.1.2 IP Configuration

Description

Use this command to configure IP basic settings, control IP interfaces, and IP routes. A maximum number of eight interfaces are supported. The maximum number of routes is 32.

```
ip name-server [ <order> ] { <v_ipv4_ucast> | { <v_ipv6_ucast> [ interface vlan
<v_vlan_id_static> ] } | dhcp [ ipv4 | ipv6 ] [ interface vlan <v_vlan_id_dhcp> ] }
```

	Argument	Description
Parameter	<order>	Preference of DNS server. Default selection is 0.
	<v_ipv4_ucast>	A valid IPv4 unicast address
	<v_ipv6_ucast>	A valid IPv6 unicast address
	dhcp	Dynamic Host Configuration Protocol

.....continued		
	Argument	**Description**
Default	No DNS server configured	
Mode	Global Configuration mode	
Usage	Set DNS for resolving domain names. Use the `no` version of the command to return to default.	

Example	1. DNS Server 0 setting is derived from any DHCPv4 VLANs-ID.
	`(config)# ip name-server 0 dhcp`
	2. DNS Server 1 configured as a static IPv4 address.
	`(config)# ip name-server 1 192.168.0.10`
	3. DNS Server 1 setting is derived from DHCPv4 VLANs-ID 1.
	`(config)#ip name-server 1 dhcp ipv4 interface vlan 1`	

Description
Use this command to add IPv4 and IPv6 interfaces.

```
ip address { { <address> <netmask> } | { dhcp [ fallback <fallback_address>
<fallback_netmask> [ timeout <fallback_timeout> ] ] [ client-id { <port_type>
<client_id_interface> | ascii <ascii_str> | hex <hex_str> } ] [ hostname <hostname> ] } }
```

```
ipv6 address <subnet>
```

```
ipv6 address { autoconfig | dhcp [ rapid-commit ] }
```

	Argument	**Description**
Parameter	`<address>`	IPv4 address
	`<netmask>`	IP netmask
	`dhcp`	Enable Dynamic Host Configuration Protocol
	`fallback`	DHCP fallback settings
	`client-id`	DHCP client identifier
	`hostname`	DHCP host name
	`<subnet>`	IPv6 prefix x:x::y/z
	`autoconfig`	Enable IPv6 Stateless Auto-configuration
	`rapid-commit`	Enable DHCPv6 client Rapid-Commit option
Default	NA	
Mode	VLAN Interface Configuration mode	
Usage	Add VLAN interface and set all IPv4 and IPv6 parameters. Use the `no` version of the command to disable the selected VLAN interface. To completely remove it, use `no interface vlan <id>` from the Global Configuration mode.	

Example	1. Set VLAN2 static IP address to 192.168.1.50 mask length 24.
	`(config)#interface vlan 2`
	`(config-if-vlan)# ip address 192.168.1.50 255.255.255.0`
	2. Add VLAN 3 and set it to get IP address from DHCP using MAC of port 1 as Client ID with a hostname test.
	`(config)#interface vlan 3`
	`(config-if-vlan)# ip address dhcp client-id GigabitEthernet 1/1 hostname test`	

Description
Use this command to add new IP route.

```
ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw> [ <distance> ]
```

	Argument	Description
Parameter	<v_ipv4_addr>	Network
	<v_ipv4_netmask>	Netmask
	<v_ipv4_gw>	Gateway
	<distance>	Distance value for this route
Default	NA	
Mode	Global Configuration mode	
Usage	To route all unknown destination IP to default gateway, use the following parameters: Network = 0.0.0.0 Netmask = 0.0.0.0 Distance = 1 To remove the route, use the `no ip route` command with all parameters for the selected route.	

Example	1. Add IP route to gateway 192.168.1.1.
	`(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1 1`
	2. Remove IP route.
	`(config)#no ip route 0.0.0.0 0.0.0.0 192.168.1.1`	

3.1.3 SNMP Configuration

Description
Use this command to enable/disable the SNMP server and the set the Engine ID.

```
snmp-server
```

```
snmp-server engine-id local <engineID>
```

	Argument	Description
Parameter	<engineID>	local engine ID
Default	NA	
Mode	Global Configuration mode	
Usage	Enable SNMP server and specify engine ID. Use the `no` version of the command to disable SNMP.	

Example	Enable SNMP.
	`# configure terminal`
	`(config)# snmp-server engine-id local 800019cb030200c1966887`	

Description
Use this command for Trap Destination and Source configuration.

```
snmp-server trap <source_name> [ id <filter_id> ] [ <oid_subtree> { include | exclude } ]
```

	Argument	Description
Parameter	<source_name>	Name of the event. Possible options are: alarmTrapStatus, authenticationFailure, coldStart, entConfigChange, ipTrapGlobalsMain, ipTrapInterfacesLink, linkDown, linkup, lldpRemTablesChange, newRoot, psecTrapGlobalsMain, psecTrapInterfaces, topologyChange, warmStart.
	<filter_id>	Trap source filter ID
	<oid_subtree>	OID to use as index filter
Default	NA	
Mode	Global Configuration mode	
Usage	Configure SNMP source. Use the no version of the command to delete the entry.	

Example	Add **Remote SNMP client was trying to access the unit using invalid username/password values** event to the trap source configuration.
	`# configure terminal`
	`(config)# snmp-server trap authenticationfailure`	

Description
Use this command to configure the SNMP community table used as a part of the SNMP group configuration.

```
snmp-server community <v3_comm> [ { ip-range <v_ipv4_addr> <v_ipv4_netmask> | ipv6-range
<v_ipv6_subnet> } ] { <v3_sec> | encrypted <v3_sec_enc> }
```

	Argument	Description
Parameter	<v3_comm>	Community Name to map to the SNMP Groups configuration. String length is 1–32 and valid ASCII characters range is 33–126.
	ip-range <v_ipv4_addr> <v_ipv4_netmask>| ipv6-range <v_ipv6_subnet>	Indicates SNMP access source address. A range of source addresses can be used to restrict source subnet, when combined with source netmask.
	<v3_sec> | encrypted <v3_sec_enc>	Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1–32 and the allowed content is ASCII characters 33–126.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure SNMP community. Use the no version of the command to delete it.	

Example	Create SNMP community named **c-name** with community secret **secret**.
	`# configure terminal`
	`(config)# snmp-server community c-name secret`	

Description
Use this command to configure SNMPv3 user.

```
snmp-server user <username> engine-id <engineID> [ { md5 { <md5_passwd> | { encrypted
<md5_passwd_encrypt> } } | sha { <sha_passwd> | { encrypted <sha_passwd_encrypt> } } } [ priv
{ des | aes } { <priv_passwd> | { encrypted <priv_passwd_encrypt> } } ] ]
```

	Argument	Description
Parameter	<username>	User name. String length is 1-32 and valid ASCII characters range is 33–126.
	<engineID>	Octet string. Must contain an even number (in hexadecimal format) between 10–64 digits.
	md5 <md5_passwd>	Authentication protocol MD5 and password length is 8–32. ASCII characters are in the range of 33–126.
	sha <sha_passwd>	Authentication protocol SHA and password length is 8–40. ASCII characters are in the range of 33–126.
	priv { des | aes }	Privacy protocol DES or AES.
	<priv_passwd>	Privacy password length is 8–32. ASCII characters are in the range of 33–126.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure SNMPv3 user. Use the no version of the command to delete it.	
Example	Add SNMPv3 user testuser with authentication protocol MD5 and password testpassword. # configure terminal (config)# snmp-server user testuser engine-id 800019ab12345 md5 testpassword	

Description
Use this command to configure SNMP group-name based on Security Model and Security name.

```
snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>
```

	Argument	Description
Parameter	v1 | v2c | v3	Security model the entry must belong to.
	<security_name>	One of the security names created in SNMP Community for v1 and v2c or one of the SNMPv3 users.
	<group_name>	Group name. String length is 1–32 and valid ASCII characters range 33–126.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure SNMP group name. Use the no version of the command to delete it.	
Example	Configure SNMPv2 security model and group. # configure terminal (config)# snmp-server security-to-group model v2c name public group ro_group	

Description
Use this command to configure which SNMP OiDs must be included/excluded from the entire SNMP OiD tree.

```
snmp-server view <view_name> <.oid_subtree> { include | exclude }
```

	Argument	Description
Parameter	<view_name>	A string identifying the view name that this entry should belong to. The allowed string length is 1–32, and the allowed content is ASCII characters from 33–126.

.....continued		
	Argument	**Description**
	<.oid_subtree>	OiD defining the root of the subtree to add to the named view. String length is 1–128. Allowed string content is number or asterisk (*).
Default	NA	
Mode	Global Configuration mode	
Usage	Configure SNMP View OiD-range. Use the no version of the command to delete it.	

Example	Create SNMP view OiD-range named **mib-ii** with access to all SNMP OiDs exept for MIB-II system branch .1.3.6.1.2.1.1.
	`# configure terminal`
	`(config)# snmp-server view mib-ii .1.3.6.1.2.1.1 excluded`	

Description
Use this command to configure SNMP access.

```
snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv }
[ read <view_name>] [ write <write_name>]
```

	Argument	**Description**
Parameter	<group_name>	Group name previously configured by security-to-group command. String length is 1–32 and valid ASCII characters range 33–126.
	model {v1 | v2c | v3 | any}	Security model the entry must belong to.
	level {auth | noauth | priv}	Security level. authNoPriv, noAuthNoPriv, authPriv
	read <view_name>	Name of the MIB view defining the MIB objects for which this request may read OiD values.
	write <write_name>]	Name of the MIB view defining the MIB objects for which this request may set OiD new values.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure SNMP group name. Use the no version of the command to delete it.	

Example	Configure SNMPv2 access.
	`# configure terminal`
	`(config)# snmp-server access ro_group model v2c level noauth read mib-ii`	

3.1.4 NTP Configuration

This command configures the unit NTP servers IP. The NTP server updates the unit with the correct Greenwich Mean Time (GMT).

Description
Use this command to enable or disable the NTP server and specifies its parameters. Up to five NTP servers can be configured.

```
ntp
```

```
ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }
```

	Argument	Description
Parameter	<index_var>	NTP Server index (1–5)
	<ipv4_var>	IPv4 address of NTP server
	<ipv6_var>	IPv6 address of NTP server
	<name_var>	Domain name of NTP server
Default	NA	
Mode	Global Configuration mode	
Usage	Enable NTP server by entering ntp command. Use a no version of the command to disable it. Specify the parameters of NTP server by entering ntp server command. Use a no version of the command to delete the specified NTP server.	
Example	1. Add NTP server 1 with IP address 192.168.1.2. (config)#ntp server 1 ip-address 192.168.1.2 2. Add NTP server 2 with domain name ntp.microsemi.com. (config)#ntp server 2 ip-address ntp.microsemi.com 3. Enable NTP server (config)#ntp	

3.1.5 Time Configuration

Use this command to configure unit local time zone and daylight saving.

Description
Configures the time zone.

```
clock timezone <word_var> <hour_var> [ <minute_var> [ <subtype_var> ] ]
```

	Argument	Description
Parameter	<word_var>	Name of time zone up to 16 characters. Use (“) for null input.
	< hour_var >	Hours offset from UTC −23–23.
	<minute_var>	Minutes offset from UTC 0–59.
	<subtype_var>	Sub type of time zone 0–9.
Default	(UTC) Coordinated Universal Time	
Mode	Global Configuration mode	
Usage	Specify the time zone and offsets from UTC. Use the no form of the command to return to default	
Example	Configure Eastern time zone with −05:00 from UTC (config)#clock timezone Eastern -05 0	

Description
Use this command to configure daylight savings time.

```
clock summer-time <word16>
```

```
date [ <start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var>
<end_date_var> <end_year_var> <end_hour_var> [ <offset_var> ] ]
```

```
clock summer-time <word16>
```

```
 recurring [ <start_week_var> <start_day_var> <start_month_var> <start_hour_var>
<end_week_var> <end_day_var> <end_month_var> <end_hour_var> [ <offset_var> ] ]
```

	Argument	Description
Parameter	<word16>	Name of time zone in summer up to 16 characters. Use “ for null input
	<start_month_var>	Month to start (1–12)
	<start_date_var>	Date to start (1–31)
	<start_year_var>	Year to start (2000–2097)
	<start_hour_var>	Time to start (hh:mm)
	<end_month_var>	Month to end (1–12)
	<end_date_var>	Date to end (1–31)
	<end_year_var>	Year to end (2000–2097)
	<end_hour_var>	Time to end (hh:mm)
	<offset_var>	Offset to add in minutes (1–1439)
	<start_week_var>	Week number to start (1–5)
	<start_day_var>	Weekday to start (1–7)
	<end_week_var>	Week number to end (1–5)
	<end_day_var>	Weekday to end (1–7)
Default	Daylight savings time mode disabled	
Mode	Global Configuration mode	
Usage	Configure summer (daylight savings) time in absolute non-recurring mode (date) and recurring mode (recurring). Use the no form of the command to return to default.	
Example	Configure non-recurring Daylight Savings Time to start on March 10, 2019 at 02:00 AM and finish on November 3, 2019 at 02:00 AM. `(config)#clock summer-time '' date 3 10 2019 02:00 11 3 2019 02:00`	

3.1.6 System Log Configuration

Use this command to configure SysLog Server IP address or domain name. When the mode operation is enabled, the syslog message sends out to syslog server. The syslog protocol is based on the UDP communication and received on UDP port 514. The syslog server does not send acknowledgments back to sender, as UDP is a connectionless protocol and does not provide acknowledgments. The syslog packet always sends out even if the syslog server does not exist.

Description

System Log configuration commands.

```
logging on
```

```
logging host { <ipv4_addr> | <domain_name> }
```

```
logging level { informational | notice | warning | error }
```

	Argument	Description
Parameter	<ipv4_addr>	The IPv4 address of the log server.
	<domain_name>	A valid name consists of a sequence of domain labels separated by (.). Each domain label starts and ends with an alphanumeric character and might also contain (-) characters. The length of a domain label must be 63 characters or less.
	Informational	Severity 6: Informational messages
	Notice	Severity 5: Normal but significant condition

.....continued		
	Argument	**Description**
	Warning	Severity 4: Warning conditions
	Error	Severity 3: Error conditions
Default	NA	
Mode	Global Configuration mode	
Usage	Enable SysLog server, specifies its address and the level of messages that are sent to it. Use the `no logging on` command to disable SysLog server.	

Example	1. Enable SysLog server at 192.168.0.1 with Warning level messages.
	`(config)#logging on`
	`(config)#logging host 192.168.0.1`
	`(config)#logging level warning`
	2. Disable SysLog server
	`(config)#no logging on`	

3.1.7 Monitor unsaved running-config Configuration

Description
Use this command to enable or disable monitoring modified unsaved `running-config`.

```
prod monitor-running-config-changes
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	Global Configuration mode	
Usage	Enable monitoring modified unsaved running-config. Use the `no` version of the command to disable it.	

Example	Enable monitoring
	`# configure terminal`
	`(config)# prod monitor-running-config-changes`	

3.2 Green Ethernet—Configuration Commands

Energy Efficient Ethernet (EEE) is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up.

The switch can be set to optimize EEE for either best power saving or least traffic latency.

3.2.1 Green Ethernet Port Power Savings Configuration

Description
Sets if EEE must be optimized for least traffic latency or least power consumption.

```
green-ethernet eee optimize-for-power
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	Global Configuration Mode	
Usage	Set the switch to optimize EEE for best power saving. Use the `no` version of the command to optimize for least traffic latency.	

Example	Optimize EEE for best power saving.
	`# configure terminal`
	`(config)# green-ethernet eee optimize-for-power`	

3.2.2 Green Ethernet Port Configuration

Description
For 1G or 100 Mbit full duplex mode ports, configure ActiPHY (lowering the power for a port when there is no link), PerfectReach (works by determining the cable length and lowering the power for ports with short cables), and enable/disable EEE and EEE Urgent Queues (set Queues set activate transmission of frames when data is available).

```
green-ethernet energy-detect
```

```
green-ethernet short-reach
```

```
green-ethernet eee
```

```
green-ethernet eee urgent-queues [ <urgent_queue_range_list> ]
```

	Argument	Description
Parameter	`<urgent_queue_range_list>`	EEE Interface. Valid range 1–8.
Default	None	
Mode	Port List Interface mode	
Usage	Configure ActiPHY, PerfectReach, EEE and EEE Urgent Queues. Use the no version of the command to revert to default.	

Example	1. Configure for port 1 ActiPHY and EEE enabled and set EEE Urgent Queues to 1, 2, 3, and 4.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# green-ethernet energy-detect`
	`(config-if)# green-ethernet eee`
	`(config-if)# green-ethernet eee urgent-queues 1-4`	

3.3 Ports Configuration Commands

These commands configure Port Speed, Advertise Duplex, Advertise Speed, Flow Control, PFC (Priority Flow Control), Maximum Frame Size, Excessive Collision Mode, and Frame Length Check.

Description
Use this command to enable/disable the Ethernet port (has no effect on PoE power).

```
shutdown
```

	Argument	Description
Parameter	—	—
Default	NA	
Mode	Port List Interface configuration mode.	
Usage	Use the command to disable the specified interface. Use `no` form of this command to enable the interface.	

Example	1. Disable port 1
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# shutdown`
	2. Disable ports 1 through 4.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1-4`
	`(config-if)# shutdown`
	3. Enable all ports.
	`# configure terminal`
	`(config)# interface *`
	`(config-if)# no shutdown`	

Description
Use this command to configure the port speed.

```
speed { 1000 | 100 | 10 | auto }
```

	Argument	Description
Parameter	10	10 Mbps
	100	100 Mbps
	1000	1000 Mbps (1 Gbps)
	auto	Auto negotiation
Default	Mode	
	Port List Interface mode	
Usage	Use to set the speed of the specified interface.	

Example	1. Set speed for port 1 to 100 Mbps
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# speed 100`
	2. Set all ports to 1 Gbps
	`# configure terminal`
	`(config)# interface *`
	`(config-if)# speed 1000`	

Description
Use this command to configure the Interface Duplex mode.

```
duplex { half | full | auto }
```

	Argument	Description
Parameter	half	Forced half duplex
	full	Forced full duplex
	auto	Auto negotiation of duplex mode.
Default	All ports are set to Auto.	
Mode	Port List Interface mode	
Usage	Use to set the duplex mode of the specified interface. Use the `no` form of the command to set duplex to default.	

Example	1. Set duplex for port 1 to half
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# duplex half`
	2. Set all ports to 1 Gbps
	`# configure terminal`
	`(config)# interface *`
	`(config-if)# speed 1000`	

Description
Use this command to configure flow control for the interface.

Note: Slow temporarily packet transition upon request, or for packet reception, signal the remote transmitter to slow down temporarily its packet transition when Switch reception buffer is full.

Both PFC and Flow control cannot be enabled on the same port.

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

```
priority-flowcontrol prio <prio>
```

	Argument	Description
Parameter	ON	Enable flow control.
	OFF	Disable flow control.
	`<prio>`	Range of priorities (for example, 0–4, 7)
Default	All ports flow control **receive** and **send** is OFF. Priority Flow Control is OFF.	
Mode	Port List Interface mode	
Usage	Use this commant to set the flow control and PFC for the interface. Use the `no` form of the command to return to defaults.	

.....continued		
	Argument	**Description**

Example	1. Enable flow control for port 1.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# flowcontrol on`
	2. Enable priority flow control with 0–3 priorities for all ports.
	`# configure terminal`
	`(config)# interface *`
	`(config-if)# priority-flowcontrol prio 0-3`	

Description
Use this command to specify maximum Ethernet frame size for the interface.

```
mtu <max_length>
```

	Argument	**Description**
Parameter	`<max_length>`	Maximum frame size in bytes (1518–10240 bytes)
Default	All ports mtu 10240 bytes	
Mode	Port List Interface mode	
Usage	Use to set the maximum frame size for the interface. Use the `no` form of the command to return to defaults.	

Example	1. Set mtu for port 1 to 1518.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# mtu 1518`
	2. Set mtu for all ports to 1518.
	`# configure terminal`
	`(config)# interface *`
	`(config-if)# mtu 1518`	

Description
Use this command to configure port transmit collision behavior.

```
excessive-restart
```

	Argument	**Description**
Parameter	NA	NA
Default	Discard frame after 16 collisions.	
Mode	Port List Interface mode	
Usage	Use to set the maximum frame size for the interface. Use the `no` form of the command to return to defaults.	

.....continued		
	Argument	**Description**

Example	1. Restart backoff algorithm after 16 collisions for port 1.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# excessive-restart`
	2. Discard frame after 16 collisions for all ports.
	`# configure terminal`
	`(config)# interface *`
	`(config-if)# no excessive-restart`	

Description
Use this command to configure if frames with incorrect frame length in the EtherType/Length field are dropped.

```
frame-length-check
```

	Argument	**Description**
Parameter	NA	NA
Default	None	
Mode	Port List Interface mode	
Usage	Drop frames with mismatch between EtherType/Length field and actual payload size. Use the `no` form of the command to disable frame check.	

Example	1. Disable frame length check for port 1.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# no frame-length-check`
	2. Enable frame length check for all ports.
	`# configure terminal`
	`(config)# interface *`
	`(config-if)# frame-length-check`	

3.4 Connectivity Fault Management (CFM) Configuration

CFM is a standard defined by IEEE® 802.1ag. It defines protocols and practices for Operations, Administration, and Maintenance (OAM).

3.4.1 CFM Global Configuration

Description
Use this command for CFM Global configuration.

```
cfm sender-id-tlv { disable | chassis | management | chassis-management }
```

```
cfm port-status-tlv { disable | enable }
```

```
cfm interface-status-tlv { disable | enable }
```

```
cfm organization-specific-tlv { disable | enable oui <oui> subtype <subtype> value <value> }
```

	Argument	Description
Parameter	`disable`	Do not send Sender ID, Port Status, Interface Status, or Organization Specific TLVs in CCMs generated by this switch.
	`chassis`	Enable Sender ID TLV and send Chassis ID (MAC Address).
	`management`	Enable Sender ID TLV and send Management address (IPv4).
	`chassis-management`	Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4).
	`enable`	Include Port Status, Interface status, or Organization-Specific TLVs in PDUs.
	`<oui>`	OUI transmitted with the Organization-Specific TLVs. Enter as 6 characters 0–9, a–f (XX-XX-XX).
	`<subtype>`	Subtype transmitted with the Organization-Specific TLV. It can be any value in range of 0–255.
	<value>	Value transmitted in the Organization-Specific TLVs. Value is a printable character string of length 0–63.
Default	None	
Mode	Global Configuration mode	
Usage	Configure CFM Global parameters	

Example	1. Enable Sender ID TLV and send Chassis ID.
	`(config)# cfm sender-id-tlv chassiscf`
	2. Send Organization Specific TLV with OUI, subtype and value.
	`(config)# cfm organization-specific-tlv enable oui 12-34-56 subtype 1 value “test”`	

3.4.2 CFM Domain Configuration

Description
Use these commands for CFM Domain configuration.

```
cfm domain <md_name>
```

```
format { none | string <name> }
```

```
level <level>
```

```
sender-id-tlv { disable | chassis | management | chassis-management | defer }
```

```
port-status-tlv { disable | enable | defer }
```

```
interface-status-tlv { disable | enable | defer }
```

```
organization-specific-tlv { disable | defer }
```

	Argument	Description
Parameter	<md_name>	Create CFM Maintenance Domain with name value as a single word which begins with an alphabetic letter A-Z or a-z with length 1–15.
	all	All CFM domains
	none	Not present (type 1)
	<name>	ASCII string from 1 to 43 characters long (type 4).
	<level>	MEG level of this domain. Valid values are restricted to 0–7.
	disable	Do not send Sender ID, Port Status, Interface Status or Organization Specific TLVs in CCMs generated by this switch.
	chassis	Enable Sender ID TLV and send Chassis ID (MAC Address).
	management	Enable Sender ID TLV and send Management address (IPv4).
	chassis-management	Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4).
	defer	Let the global configuration decide.
	enable	Include Port Status, Interface status, or Organization-Specific TLVs in PDUs.
Default	None	
Mode	Global Configuration mode and CFM Domain configuration mode.	
Usage	Create the CFM Domain and configure its parameters. Use the no version of the command to delete the specific domain by name or use parameter **all** to delete all CFM domains.	

Example	1. Create CFM domain test.
	`(config)# cfm domain test`
	2. Set the format to string with the name teststring and level 5.
	`(config-cfm-dmn)# format string "teststring"`
	`(config-cfm-dmn)# level 5`	

3.4.3 CFM Service Configuration

Description
Use these commands for CFM Service configuration.

```
service <ma_name>
```

```
format { string <format_string> | integer <format_integer> | primary-vid | icc
<format_icc_string> | icc-cc <format_icc_cc_string> }
```

```
type { port | vlan <vid> }
```

```
continuity-check interval { 3.3ms | 10ms | 100ms | 1s | 10s | 1min | 10min }
```

```
sender-id-tlv { disable | chassis | management | chassis-management | defer }
```

```
port-status-tlv { disable | enable | defer }
```

```
interface-status-tlv { disable | enable | defer }
```

```
organization-specific-tlv { disable | defer }
```

	Argument	Description
Parameter	<ma_name>	Create CFM Service with name value as a single word which begins with an alphabetic letter A–Z or a–z with length 1–15.
	all	All CFM services.
	<format_string>	Length must be in range of 1–44. Contents must be in range of 32–126.
	<format_integer>	Integer in range 0–65535
	<format_icc_string>	ITU-T ICC-based format (type 32).
	<format_icc_cc_string>	ITU-T ICC-CC-based format (type 33).
	<vid>	This is MA's primary VID.
	disable	Do not send Sender ID, Port Status, Interface Status, or Organization Specific TLVs in CCMs generated by this switch.
	chassis	Enable Sender ID TLV and send Chassis ID (MAC Address).
	management	Enable Sender ID TLV and send Management address (IPv4).
	chassis-management	Enable Sender ID TLV and send Chassis ID (MAC Address) and Management Address (IPv4).
	defer	Let the global configuration decide.
	enable	Include Port Status, Interface status, or Organization-Specific TLVs in PDUs.
Default	None	
Mode	CFM Service configuration mode.	
Usage	Create CFM Service and configure its parameters. Use the no version of the command to delete the specific service by name or use parameter **all** to delete all CFM services.	

.....continued		
	Argument	**Description**

Example	1. Create CFM service testservice under CFM domain test.
	`(config)# cfm domain test`
	`(config-cfm-dmn)# service testservice`
	2. Set the format to Primary VID with CCM interval 10 ms.
	`(config-cfm-dmn-svc)# format primary-vid`
	`(config-cfm-dmn-svc)# continuity-check interval 10ms`	

3.4.4 CFM MEP Configuration

Description
Use these commands for CFM Mep configuration.

```
mep <mepid>
```

```
direction { up | down }
```

```
interface <port_type> <port>
```

```
vlan { inherit | <vid> }
```

```
pcp <pcp>
```

```
smac <mac>
```

```
alarm-level <alarm_level>
```

```
alarm-time-present <alarm_time_present_ms>
```

```
alarm-time-absent <alarm_time_absent_ms>
```

```
continuity-check
```

```
admin-state { enable | disable }
```

```
remote mep <rmepid>
```

	Argument	**Description**
Parameter	`<mepid>`	The identification of this MEP. Must be an integer [1…8091].
	`up | down`	Set if this MEP is an Up-MEP or a Down-MEP.
	`<port_type> <port>`	Port on which this MEP resides.
	`inherit | <vid>`	Inherit from the service's type or use this VLAN ID.
	`<pcp>`	Choose PCP value in PDUs' VLAN tag. Not used if untagged.
	`<mac>`	Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX.

.....continued		
	Argument	**Description**
	<alarm_level>	If a defect is detected with a priority higher than this level, a fault alarm notification is generated. Valid range is 1–6 with 1 indicating that any defect can cause a fault alarm and 6 indicating that no defect can cause a fault alarm.
	<alarm_time_present_ms>	The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.
	<alarm_time_absent_ms>	The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.
	<rmepid>	Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID.
Default	None	
Mode	CFM Service configuration mode.	
Usage	Configure CFM MEP parameters. Use the no version of the command to delete the specific service by name or use parameter **all** to delete all CFM services.	

Example	Configure CFM MEP with ID1 on port 2.
	`(config)# cfm domain test`
	`(config-cfm-dmn)# service testservice`
	`(config-cfm-dmn-svc)# mep 1`
	`(config-cfm-dmn-svc-mep)# interface GigabitEthernet 1/2`	

3.5 Automatic Protection Switching (APS) Configuration

Description
Use this command to create and configure an APS instance.

```
aps <inst>
```

```
mode { 1-for-1 | bidirectional-1-plus-1 | unidirectional-1-plus-1 [ tx-aps ] }
```

```
smac <mac>
```

```
level <level>
```

```
vlan { untagged | <vid> [ pcp <pcp> ] }
```

```
revertive
```

```
wait-to-restore <wtr>
```

```
hold-off-time <hold_off>
```

```
admin-state { enable | disable }
```

```
protect interface <port_type> <port>
```

```
working interface <port_type> <port>
```

```
protect sf-trigger { link | { mep domain <md_name> service <ma_name> mep-id <mepid> } }
```

```
working sf-trigger { link | { mep domain <md_name> service <ma_name> mep-id <mepid> } }
```

	Argument	Description
Parameter	<inst>	APS instance number 1–6.
	1-for-1	Source determines the port into which the traffic goes.
	bidirectional-1-plus-1	Traffic goes into both ports and sink selects based on local defects and APS PDUs received from the far end.
	unidirectional-1-plus-1	Traffic goes into both ports and sink selects exclusively based on local defects.
	tx-aps	Choose if this end transmits APS PDUs. Only used for 1+1, unidirectional.
	<mac>	Source MAC address used in L-APS PDUs. This must be a unicast address. Format is XX: XX: XX: XX: XX: XX.
	<level>	Set the MD/MEG level used in L-APS PDUs (0–7).
	untagged | <vid>	Do not insert a VLAN tag in the L-APS PDUs or insert the VLAN ID used in the L-APS PDUs.
	<pcp>	Choose a PCP to be used in the 802.1Q tag (0–7).
	<wtr>	Wait-To-Restore (WTR) describes how many seconds you must wait before restoring to the working port after a fault condition has cleared. Valid range is 1–720.

.....continued		
	Argument	**Description**
	`<hold_off>`	Hold-off timer value measured in milliseconds. It must be in multiples of 100 ms. Range is 0–10000.
	`enable | disable`	Enable or disable this APS instance.
	`<port_type> <port>`	The port to which this flow is attached.
	`link | { mep domain <md_name> service <ma_name> mep-id <mepid>`	Protect Interface Link state is used as signal-fail trigger, or a MEP installed on protect interface is used as signal-fail trigger. Specify MEP's domain name and service name within the domain and MEP's ID.
Default	None	
Mode	APS mode	
Usage	Configure APS parameters. Use the `no` version of the command to delete the specific APS instance or use parameter **all** to delete all APS instances.	

Example	Create APS instance 1, set the mode to bidirectional-1-plus-1, and attach to port 2.
	`(config)# aps 1`
	`(config-aps)# mode bidirectional-1-plus-1`
	`(config-aps)# protect interface GigabitEthernet 1/2`	

3.6 Ethernet Ring Protection Switching (ERPS) Configuration

Description
Use this command to create and configure an ERPS Instance.

```
erps <inst>
```

```
erps <inst> clear
```

```
version { v1 | v2 }
```

```
ring-type { major | sub-ring [ virtual-channel ] | interconnected-sub-ring { connected-ring
<connected_ring_inst> [ virtual-channel ] [ propagate-topology-change ] } }
```

```
port0 interface <port_type> <port>
```

```
port0 sf-trigger { link | { mep domain <md_name> service <ma_name> mep-id <mepid> } }
```

```
port0 smac <mac>
```

```
port1 interface <port_type> <port>
```

```
port1 sf-trigger { link | { mep domain <md_name> service <ma_name> mep-id <mepid> } }
```

```
port1 smac <mac>
```

```
ring-id <ring_id>
```

```
node-id <node_id>
```

```
level <level>
```

```
control-vlan <vid> [ pcp <pcp> ]
```

```
revertive
```

```
guard-time <guard_time>
```

```
wait-to-restore <wtr>
```

```
hold-off-time <hold_off>
```

```
admin-state { enable | disable }
```

```
protected-vlans <vlan_list>
```

```
rpl { owner | neighbor } { port0 | port1 }
```

	Argument	Description
Parameter	`<inst>`	ERPS instance number 1–6.
	`{ v1 | v2 }`	Use version 1 or 2 of the R-APS protocol
	`major`	Make this a major ring, which always has two ring ports.
	`sub-ring [ virtual-channel ]`	Make this a non-interconnected sub-ring, which has two ring ports. Configure this sub-ring with a R-APS virtual channel.
	`interconnected-sub-ring`	Make this an interconnected sub-ring, which has only one ring port (port0) but connects to a major ring.
	`connected-ring <connected_ring_inst>`	An interconnected sub-ring points to another ring with two ring ports. The ERPS instance number of the connected ring that this interconnected sub-ring connects to
	`propagate-topology-change`	If a topology-change occurs on this interconnected sub-ring, the connected ring also flushes its FDB.
	`<port_type> <port>`	Port type and ID assigned to ring port0 and/or ring port1.
	`link | { mep domain <md_name> service <ma_name> mep-id <mepid>`	Protect interface link state is used as signal-fail trigger or a MEP installed on protect interface is used as signal-fail trigger. Specify MEP's domain name and service name within the domain and MEP's ID.
	`<mac>`	Source MAC address used in R-APS PDUs. This must be a unicast address. Format is XX:XX:XX:XX:XX:XX.
	`<ring_id>`	Ring ID (1-239). If using G.8032 version 1, this must be 1.
	`<node_id>`	Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring. This must be a unicast address. Format is XX:XX:XX:XX:XX:XX
	`<level>`	Set the MD/MEG level used in R-APS PDUs (0–7).
	`<vid>`	The VLAN on which R-APS PDUs are transmitted and received on the ring ports.
	`<pcp>`	The PCP value used in the VLAN tag of the R-APS PDUs. (0–7).
	`<guard_time>`	Guard time in ms. Valid range is 10 ms–2000 ms.
	`<wtr>`	Wait-to-Restore time in seconds. Valid range 1s–720s.
	`<hold_off>`	Hold-off timer value measured in milliseconds. This must be in multiples of 100 ms. Range is 0–10000.
	`enable | disable`	Enable or disable this ERPS instance.
	`<vlan_list>`	VLANs which are protected by this ring instance. At least one VLAN must be protected. Specify as a comma separated list of vlan numbers or VLAN ranges. For example, 1, 4, 7, 30–70.
	`owner | neighbor`	This switch is RPL owner or the neighbor for the ring. Use the `no` version of the command to configure instance to be normal ring node.
Default	None	
Mode	ERPS mode	
Usage	Configure ERPS parameters. Use the `no` version of the command to delete the specific ERPS instance or use parameter **all** to delete all ERPS instances.	

Example	Create ERPS instance 1 version v1 and ring type major.
	`(config)# erps 1`
	`(config-erps)# version v1`
	`(config-erps)# ring-type major`	

3.7 DHCPv4 Snooping Configuration

Description
Use this command to enable or disable the DHCP snooping mode operation and the port mode.

```
ip dhcp snooping
```

```
ip dhcp snooping trust
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	Global Configuration mode and Port List Configuration mode.	
Usage	Globally enable DHCP snooping. Use the `no` form of this command to globally disable DHCP snooping. Configure a port as trusted for DHCP snooping purposes. Use the `no` form of this command to configure a port as untrusted.	

Example	1. Enable dhcp snooping.
	`# configure terminal`
	`(config)# ip dhcp snooping`
	2. Enable dhcp snooping trust on port 1.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# ip dhcp snooping trust`	

3.8 DHCPv6 Snooping Configuration

Description
Use this command to enable or disable the DHCPv6 Snooping mode operation and configure the Port Trust mode.

```
ipv6 dhcp snooping
```

```
ipv6 dhcp snooping nh-unknown { drop | allow }
```

```
ipv6 dhcp snooping trust
```

	Argument	Description
Parameter	`drop`	Drop packets with unknown IPv6 extension headers.
	`allow`	Allow packets with unknown IPv6 extension headers.
Default	NA	
Mode	Global Configuration mode and Port List Configuration mode.	
Usage	Globally enable DHCP snooping. Use the `no` form of this command to globally disable DHCP snooping. Configure a port as trusted for DHCPv6 snooping purposes. Use the `no` form of this command to configure a port as untrusted.	

.....continued		
	Argument	**Description**

Example	1. Enable dhcpv6 snooping and allow packets with unknown IPv6 extension headers.
	`# configure terminal`
	`(config)# ipv6 dhcp snooping`
	`(config)# ipv6 dhcp snooping nh-unknown allow`
	2. Enable dhcpv6 snooping trust on port 1.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# ipv6 dhcp snooping trust`	

3.9 Security Configuration

The following commands configure security settings for Switch, Network, and Authentication, Authorization and Accounting (AAA).

3.9.1 Add Local User to Switch or Change Password

Description

Use this command to add, remove, or change password of local users. Up to 20 users can be configured.

```
username { default-administrator | <input_username> } privilege <priv> password { unencrypted
<unencry_password> | encrypted <encry_password> | none }
```

	Argument	**Description**
Parameter	`<input_username>`	User name allows letters, numbers, and underscores.
	`<priv>`	User privilege level 0–15. **Note:** Use only privilege level 15.
	`<unencry_password>`	The UNENCRYPTED (Plain Text) user password. Any printable characters including space are accepted. **Note:** You do not get the Plain Text password after this command. The system always displays the ENCRYPTED password.
	`<encry_password>`	The ENCRYPTED (hidden) user password. **Note:** The ENCRYPTED password is decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.
	none	NULL password
Default	NA	
Mode	Global Configuration mode	
Usage	Add a new user for the local switch access and add/change password.	

.....continued		
	Argument	**Description**

Example	1. Add a user named usertest with unencrypted password of testuser.
	`(config)# username usertest privilege 15 password unencrypted testuser`
	2. Remove user named usertest.
	`(config)# no username usertest`
	3. Change the password of usertest to testuser123.
	`(config)# username usertest privilege 15 password unencrypted testuser123`	

3.9.2 Privilege Level Configuration

Description
The Privilege levels can be configured between 0–15 (where 0 is lowest level and 15 is highest level). Every group has an authorization Privilege level for the following subgroups—configuration read-only, configuration/execute read-write, status/statistics read-only, and status/statistics read-write (for example, for clearing of statistics).

```
web privilege group <group_name> level { [ configRoPriv <configRoPriv> ] [ configRwPriv
<configRwPriv> ] [ statusRoPriv <statusRoPriv> ] [ statusRwPriv <statusRwPriv> ] }
```

	Argument	**Description**
Parameter	`<group_name>`	Web privilege group name. Valid words: APS, Aggregation, Alarm, CFM, DHCP, DHCPv6_Client, Debug, Diagnostics, ERPS, Firmware, Green_Ethernet, IP, LACP, LLDP, Loop_Protect, MAC_Table, Miscellaneous, NTP, POE, Ports, QoS, RMirror, Security(access), Security(network), Spanning_Tree, System, UPnP, VLANs, sFlow, and uFDMA_AIL, uFDMA_CIL.
	`<configRoPriv>`	Configuration read-only level 0–15.
	`<configRwPriv>`	Configuration/Execute read/write 0–15.
	`<statusRoPriv>`	Status/statistics read-only 0–15.
	`<statusRwPriv>`	Status/statistics read/write 0–15.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure Switch Privilege levels for groups.	
Example	Set Alarm group Configuration/Execute read/write privilege level to 15. `(config)# web privilege group Alarm level configRwPriv 15`	

3.9.3 AAA Configuration

Description
The authentication allows you to configure how you are authenticated when you log into the switch through one of the management client interfaces. Each one of the interfaces can have up to three authentication servers. If the first authentication server is down, then second authentication server is accessed. Same for the third authentication server, if both the first and second authentication servers are down.

The authorization allows you to limit the CLI commands available to a user.

The accounting allows you to configure command and exec (login) accounting.

```
aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs }
[ { local | radius | tacacs } [ { local | radius | tacacs } ] ] }
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	Global Configuration mode	
Usage	Configure user authentication method for a specific management interface. Use the `no` version of the command to disable the interface.	

Example	1. Configure SSH to be first by the RADIUS server. If it is down, then authenticated by TACACS server. If the TACACS server is also down, then it is authenticated locally.
	`(config)#aaa authentication login ssh radius tacacs localconfig)# aaa authentication login ssh radius tacacs local`
	2. Disable Telnet remote access
	`(config)# no aaa authentication login telnet`	

```
aaa authorization { console | telnet | ssh }
```

```
tacacs commands <priv_lvl> [ config-commands ]
```

	Argument	Description
Parameter	`<priv_lvl>`	Privilege level is 0–15.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure authorization method for a specific management interface. Use the `no` version of the command to disable the authorization	

Example	1. Configure SSH client to use tacacs server for command authorization with priviledge level 15 and authorize configuration commands.
	`(config)# aaa authorization ssh tacacs commands 15 config-commands`
	2. Disable SSH command authorization remote access.
	`(config)# no aaa authorization ssh`	

```
aaa accounting { console | telnet | ssh }
```

```
tacacs { [ commands <priv_lvl> ] [ exec ] }
```

	Argument	Description
Parameter	`[commands <priv_lvl> ]`	All CLI commands equal and above the privilege level are accounted.
	`[ exec ]`	Only remote user login/logout is reported.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure accounting method and reporting. Use the `no` version of the command to disable accounting.	

Example	1. Configure accounting for ssh to report all CLI activity and any login/logout.
	`(config)# aaa accounting ssh tacacs commands 15 exec`
	2. Disable accounting for Telnet.
	`(config)# no aaa accounting telnet`	

3.9.4 SSH and HTTPS Configurations

Description
Use this command to configure SSH and HTTPS mode operations.

```
ip ssh
```

```
ip http secure-server
```

```
ip http secure-redirect
```

```
ip http secure-certificate { upload <url_file> [ pass-phrase <pass_phrase> ] | delete |
generate }
```

	Argument	Description
Parameter	<url_file>	Upload a certificate through URL. The supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A–Za–z), digits (0–9), dot (.), hyphen (-), and under score(_). The maximum length is 63 and hyphen must not be the first character. The file name content that only contains (.) is not allowed.
	<pass_phrase>	Privacy key pass phrase string if uploading certificate protected by a specific passphrase.
Default	NA	
Mode	Global Configuration mode	
Usage	Enable SSH and HTTPS. Use the no version of the command to disable it. Manage the HTTPS certificate (PEM format).	
Example	1. Upload the HTTPS certificate from TFTP server. (config)# ip http secure-certificate upload tftp://10.9.52.103/test_ca.pem 2. Delete current certificate. (config)# ip http secure-certificate delete	

3.9.5 Access Management Configuration

Description
Use this command to configure access management table.

```
access management
```

```
access management <access_id> <access_vid> <start_addr> [ to <end_addr> ] { [ web ] [ snmp ]
[ telnet ] | all }
```

	Argument	Description
Parameter	<access_id>	The maximum number of entries is 16
	<access_vid>	Indicates the VLAN ID for the access management entry.

.....continued		
	Argument	**Description**
	<start_addr>	Indicates the start IP unicast address for the access management entry.
	<end_addr>	Indicates the end IP unicast address for the access management entry.
	<access_id_list>	ID of access management entry
Default	NA	
Mode	Global Configuration mode	
Usage	Enable/Disable access management.	

Example	1. Enable access management ID1, VLAN ID1 from IP 10.10.01 to 10.10.0.99 for all interfaces.
	`(config)# access management 1 1 10.10.0.1 to 10.10.0.99 all`
	2. Delete access management entry 1.
	`(config)# no access management 1`	

3.9.6 RMON Statistics Configuration

Description
Configure RMON Statistics on a port.

```
rmon collection stats <id>
```

	Argument	**Description**
Parameter	<id>	Indicates the index of the entry. The range is from 1 to 65535.
Default	NA	
Mode	Port List Interface mode	
Usage	Configure Remote Monitoring Collection on an interface. Use the `no` version of the command to delete the entry.	

Example	1. Configure RMON on port 2 with ID1.
	`(config)# interface GigabitEthernet 1/2`
	`(config-if)# rmon collection stats 1`
	2. Delete RMON on port 2 with ID1.
	`(config)# interface GigabitEthernet 1/2`
	`(config-if)# no rmon collection stats 1`	

3.9.7 RMON History Configuration

Description
Use this command to configure RMON history on a port.

```
rmon collection history <id> [ buckets <buckets> ] [ interval <interval> ]
```

	Argument	**Description**
Parameter	<id>	Indicates the index of the entry. The range is from 1 to 65535.
	<buckets>	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600 and default value is 50.

.....continued		
	Argument	**Description**
	<interval>	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600 and default value is 1800 seconds.
Default	NA	
Mode	Port List Interface mode	
Usage	Configure Remote Monitoring history on an interface. Use the no version of the command to delete the entry.	

Example	1. Configure RMON history on port 2 with ID1, maximum data entries 40 and interval 1500 seconds.
	`(config)# interface GigabitEthernet 1/2`
	`(config-if)# rmon collection history 1 buckets 40 interval 1500`
	2. Delete RMON history entry ID1.
	`(config)# interface GigabitEthernet 1/2`
	`(config-if)# no rmon collection history 1`	

3.9.8 RMON Alarm Configuration

Description
Use this command to configure RMON alarm on a port.

```
rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors
| ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards
| ifOutErrors | ifOutQLen } <ifIndex> <interval> { absolute | delta } rising-threshold
<rising_threshold> <rising_event_id> falling-threshold <falling_threshold> <falling_event_id>
{ [ rising | falling | both ] }
```

	Argument	**Description**
Parameter	<id>	Indicates the index of the entry. The range is from 1 to 65535.
	ifInDiscards	The number of inbound packets that are discarded even the packets are normal.
	ifInErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
	ifInNUcastPkts	The number of broadcast and multicast packets delivered to a higher-layer protocol.
	ifInOctets	The total number of octets received on the interface, including framing characters.
	ifInUcastPkts	The number of uni-cast packets delivered to a higher-layer protocol.
	ifInUnknownProtos	The number of the inbound packets that were discarded because of the unknown or un-support protocol.
	ifOutDiscards	The number of outbound packets that are discarded event the packets is normal.
	ifOutErrors	The number of outbound packets that cannot be transmitted because of errors.
	ifOutOctets	The number of octets transmitted out of the interface, including framing characters.
	ifOutQLen	The length of the output packet queue (in packets).
	ifOutUcastPkts	The number of uni-cast packets that request to transmit.

.....continued		
	Argument	**Description**
	<ifIndex>	Indicates the port ID. If in stacking switch, the value must add 1000000*(switch ID-1). For example, if the port is switch 1 port 5, then the value is 1000005.
	<interval>	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31−1.
	<rising_threshold>	Rising threshold value (−2147483648 to 2147483647).
	<rising_event_id>	Rising event index (0–65535). If this value is zero, then no associated event is generated, as zero is not a valid event index.
	<falling_threshold>	Falling threshold value (−2147483648 to 2147483647).
	<falling_event_id>	Falling event index (0–65535). If this value is zero, then no associated event is generated, as zero is not a valid event index.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure Remote Monitoring alarm on an interface. Use the no version of the command to delete the entry.	

Example	1. Configure RMON alarm on port 3 with ID1, interval 50s, sampling directly.
	`(config)# rmon alarm 1 ifOutUcastPkts 1000003 50 absolute rising-threshold 70 1 falling-threshold 60 2 both`
	2. Delete RMON alarm entry ID1.
	`(config)# no rmon alarm 1`	

3.9.9 RMON Event Configuration

Description
Configure RMON event.

```
rmon event <id> [ log ] [ trap [ <word127> ] ] { [ description <description> ] }
```

	Argument	**Description**
Parameter	<id>	Indicates the index of the entry. The range is from 1 to 65535.
	<word127>	OBSOLETE: SNMP community string
	<description>	Indicates this event. The string length is from 0 to 127 and default is a null string.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure Remote Monitoring event. Use the no version of the command to delete the entry.	

Example	1. Configure RMON event with ID1 description test and create SNMP log entry and sent SNMP trap when the event is triggered.
	`(config)# rmon event 1 log trap description test`
	2. Delete RMON event entry ID1.
	`(config)# no rmon event 1`	

3.9.10 Port Security Configuration

Description
Use this command to configure Port Security global settings. If aging is enabled, secured MAC addresses are subject to aging with a specified period and hold time (how long a MAC address is held in the MAC table, if it has been found to violate the limit).

```
port-security aging
```

```
port-security aging time <aging_time>
```

```
port-security hold time <hold_time>
```

	Argument	Description
Parameter	<aging_time>	The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds.
	<hold_time>	Valid range is between 10 and 10000000 seconds with a default of 300 seconds.
Default	NA	
Mode	Global Configuration mode	
Usage	Enable port security aging. Use the no version of the command to disable port security aging or revert to default aging period and hold time.	

Example	1. Enable aging
	`(config)# port-security aging`
	2. Set the aging period and hold time to 600s.
	`(config)# port-security aging time 600`
	`(config)# port-security hold time 600`	

Description
Use this command to configure Port Security settings. Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode. The following are the types of violation modes:

- Protect: Do not allow more than Limit MAC addresses on the port, but take no further action.
- Restrict: If the limit is reached, then subsequent MAC addresses on the port are counted and marked as violating. These MAC addresses are removed from the MAC table when the hold time expires. At most, Violation Limit MAC addresses can be marked as violating at any given time.
- Shutdown: If the limit is reached, thenone additional MAC address causes the port to be shut down.

```
port-security
```

```
port-security maximum <limit>
```

```
port-security maximum-violation <violate_limit>
```

```
port-security violation { protect | restrict | shutdown }
```

```
port-security mac-address { [ sticky ] [ <mac> [ vlan <vlan_id> ] ] }
```

```
no port-security mac-address { [ sticky ] [ <mac> [ vlan <vlan_id> ] ] }
```

	Argument	Description
Parameter	<limit>	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4.
	<violate_limit>	The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when the Violation mode is Restrict.
	<mac>	MAC address in format XX:XX:XX:XX:XX:XX.
Default	NA	
Mode	Port List Interface mode.	
Usage	Enable port security. Use the no version of the command to disable port security or revert to default values.	

Example	1. Enable security on port 2.
	`(config)# interface GigabitEthernet 1/2`
	`(config-if)#port security`
	2. Set the violation mode to Restrict and set the violation limit to 100.
	`(config-if)# port-security violation restrict`
	`(config-if)# port-security maximum violation 100`	

3.9.11 Network Access Server (NAS) Configuration

Description
Use this command to configure the IEEE 802.1X and MAC-based authentication system settings. Globally enable/disable NAS, enable/disable Reauthentication, and set the Reauthentication Period (successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period). Set the time for retransmission of Request Identity EAPOL frames and Aging period (authentication timer inactivity). Set the Hold Time (if a client is denied access, then it is put on hold in the Unauthorized state). Globally enable/disable Guest VLAN functionality, RADIUS-server assigned QoS Class functionality, and RADIUS-server assigned VLAN functionality.

```
dot1x system-auth-control
```

```
dot1x re-authentication
```

```
dot1x authentication timer re-authenticate <v_1_to_3600>
```

```
dot1x timeout tx-period <v_1_to_65535>
```

```
dot1x authentication timer inactivity <v_10_to_100000>
```

```
dot1x timeout quiet-period <v_10_to_1000000>
```

```
dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }
```

```
dot1x guest-vlan <value>
```

```
dot1x max-reauth-req <value>
```

```
dot1x guest-vlan supplicant
```

	Argument	Description
Parameter	`<v_1_to_3600>`	Determines the period in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1s−3600s. Default is 3600.
	`<v_1_to_65535>`	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1s−65535s. Default is 30.
	`<v_10_to_100000>`	Aging period (authentication timer inactivity) can be set to a number between 10s−1000000s. Default is 300. Hold time (quiet period) can be set to a number between 10s−1000000s. Default is 10.
	`guest-vlan <value>`	Value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. Valid values are in the range of 1−4095. Default is 1
	`max-reauth-req <value>`	The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN. Valid values are in the range 1−255. Default is 2.
Default	NA	
Mode	Global Configuration mode	
Usage	Set the system global NAS parameters. Use the `no` version of the command to revert to default values.	

Example	1. Enable NAS on the switch, enable reauthentication, and set the period to 3000 seconds.
	`(config)# dot1x system-auth-control`
	`(config)# dot1x re-authentication`
	`(config)# dot1x authentication timer re-authenticate 3000`
	2. Disable NAS
	`(config)#no dot1x system-auth-control`	

Description
NAS per Port configuration. Set the port authentication mode. Enable/disable per-port state of RADIUS-assigned QoS. Enable/disable per-port state of RADIUS-assigned VLAN. Enable/Disable guest VLAN.

```
dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-
based }
```

```
dot1x radius-qos
```

```
dot1x radius-vlan
```

```
dot1x guest-vlan
```

	Argument	Description
Parameter	`force-authorized`	The switch sends one EAPOL Success frame when the port link comes up, and any client on the port is allowed network access without authentication.
	`force-unauthorized`	The switch sends one EAPOL Failure frame when the port link comes up, and any client on the port is disallowed network access.
	`auto`	Port-based 802.1X Authentication
	`single`	Single Host 802.1X Authentication
	`multi`	Multiple Host 802.1X Authentication

.....continued		
	Argument	**Description**
	mac-based	Switch authenticates on behalf of the client
Default	NA	
Mode	Port List Interface mode	
Usage	Set the port NAS parameters. Use the no version of the command to revert to default values (disabled).	

Example	1. Set port 2 to single Host 802.1X Authentication with Guest VLAN enabled.
	`(config)# interface GigabitEthernet 1/2`
	`(config-if)# dot1x port control single`
	`(config-if)# dot1x guest vlan`
	2. Change the port 2 state back to default forced authorized.
	`(config-if)#no dot1x port control`	

3.9.12 Access Control List (ACL) Ports Configuration

Description
Use this command to configure the ACL parameters of each switch port. Select the policy to apply to the port and if forwarding is permitted or denied. Specify which rate limiter to apply on the port and which port frames are redirected on. Specify the mirror, logging, shut down operation, and the port state.

```
access-list policy <policy_id>
```

```
access-list action { permit | deny }
```

```
access-list rate-limiter <rate_limiter_id>
```

```
access-list { redirect } interface { <port_type> <port_type_id> | <port_type>
[ <port_type_list> ] }
```

```
access-list mirror
```

```
access-list logging
```

```
access-list shutdown
```

```
access-list port-state
```

	Argument	**Description**
Parameter	<policy_id>	The allowed values are 0–63. The default value is 0.
	{ permit | deny }	Select if forwarding is permitted or denied. The default value is **Permit**.
	<rate_limiter_id>	The allowed values are Disabled or the values 1 through 16. The default value is **Disabled**.
	<port_type>	Gigabit Ethernet or 2.5 Gigabit Ethernet.
	<port_type_id>	Port ID in the format of switch-no/port-no.
	<port_type_list>	List of Port ID. For example, 1/1, 3–5, 2/2–4, 6.
Default	NA	
Mode	Port List Interface mode	

.....continued		
	Argument	**Description**
Usage	Set the port ACL parameters. Use the `no` version of the command to revert to default.	

Example	1. On port 2, set the policy ID1 with denied forwarding.
	`(config)# interface GigabitEthernet 1/2`
	`(config-if)# access-list policy 1`
	`(config-if)# access-list action deny`
	2. Restore the default access-list policy ID.
	`(config-if)#no access-list policy`	

3.9.13 Access Control List (ACL) Rate Limiter Configuration

Description
Use this command to configure the rate limiter for the ACL of the switch.

```
access-list rate-limiter [ <rate_limiter_list> ] { pps <pps_rate> | 100pps <pps100_rate> |
100kbps <kpbs100_rate> }
```

	Argument	**Description**
Parameter	`<rate_limiter_list>`	The rate limiter ID. The range is 1–16.
	`<pps_rate>`	pps rate value 0–99
	`<pps100_rate>`	pps rate value 0–10920
	`<kpbs100_rate>`	Kbps rate value 0–10000
Default	NA	
Mode	Global Configuration mode	
Usage	Configure the rate limiter. Use the `no` version of the command to disable ACL rate limiter.	

Example	1. Configure the access list rate limiter ID 1 pps–300 pps.
	`(config)# access-list rate-limiter 1 100pps 3`
	2. Disable ACL rate limiter.
	`(config)#no access-list rate-limiter`	

3.9.14 Access Control Entry (ACE) Configuration

Description
Use this command to configure the ACE parameters. Use the `access-list ace global configuration` command to set the access-list ace. The command without the update keyword creates or overwrites an existing ACE, and any unspecified parameter is set to its default value. Use the update keyword to update an existing ACE and only specified parameter are modified. The ACE must be ordered by an appropriate sequence, as the received frame is only hit on the first matched ACE. Use the next or last keyword to adjust the ACE's sequence order.

```
access-list ace [ update ] <ace_id> [ next { <ace_id_next> | last } ] [ ingress { interface
{ <port_type> <ingress_port_id> | <port_type> [ <ingress_port_list> ] } | any } ] [ policy
<policy> [ policy-bitmask <policy_bitmask> ] ] [ tag { tagged | untagged | any } ] [ vid
{ <vid> | any } ] [ tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3
| 4-7 | any } ] [ dmac-type { unicast | multicast | broadcast | any } ] [ frame-type
{ any | etype [ etype-value { <etype_value> | any } ] [ smac { <etype_smac> | any } ]
[ dmac { <etype_dmac> | any } ] | arp [ sip { <arp_sip> | any } ] [ dip { <arp_dip>
| any } ] [ smac { <arp_smac> | any } ] [ arp-opcode { arp | rarp | other | any } ]
[ arp-flag [ arp-request { <arp_flag_request> | any } ] [ arp-smac { <arp_flag_smac> |
any } ] [ arp-tmac { <arp_flag_tmac> | any } ] [ arp-len { <arp_flag_len> | any } ]
[ arp-ip { <arp_flag_ip> | any } ] [ arp-ether { <arp_flag_ether> | any } ] ] | ipv4
[ sip { <sipv4> | any } ] [ dip { <dipv4> | any } ] [ ip-protocol { <ipv4_protocol> |
any } ] [ ip-flag [ ip-ttl { <ip_flag_ttl> | any } ] [ ip-options { <ip_flag_options> |
```

```
any } ] [ ip-fragment { <ip_flag_fragment> | any } ] ] | ipv4-icmp [ sip { <sipv4_icmp>
| any } ] [ dip { <dipv4_icmp> | any } ] [ icmp-type { <icmpv4_type> | any } ] [ icmp-
code { <icmpv4_code> | any } ] [ ip-flag [ ip-ttl { <ip_flag_icmp_ttl> | any } ] [ ip-
options { <ip_flag_icmp_options> | any } ] [ ip-fragment { <ip_flag_icmp_fragment> |
any } ] ] | ipv4-udp [ sip { <sipv4_udp> | any } ] [ dip { <dipv4_udp> | any } ] [ sport
{ <sportv4_udp_start> [ to <sportv4_udp_end> ] | any } ] [ dport { <dportv4_udp_start>
[ to <dportv4_udp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_udp_ttl> | any } ]
[ ip-options { <ip_flag_udp_options> | any } ] [ ip-fragment { <ip_flag_udp_fragment> |
any } ] ] | ipv4-tcp [ sip { <sipv4_tcp> | any } ] [ dip { <dipv4_tcp> | any } ] [ sport
{ <sportv4_tcp_start> [ to <sportv4_tcp_end> ] | any } ] [ dport { <dportv4_tcp_start>
[ to <dportv4_tcp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_tcp_ttl> | any } ]
[ ip-options { <ip_flag_tcp_options> | any } ] [ ip-fragment { <ip_flag_tcp_fragment> |
any } ] ] [ tcp-flag [ tcp-fin { <tcpv4_flag_fin> | any } ] [ tcp-syn { <tcpv4_flag_syn>
| any } ] [ tcp-rst { <tcpv4_flag_rst> | any } ] [ tcp-psh { <tcpv4_flag_psh> | any } ]
[ tcp-ack { <tcpv4_flag_ack> | any } ] [ tcp-urg { <tcpv4_flag_urg> | any } ] ] | ipv6
[ next-header { <next_header> | any } ] [ sip { <sipv6> [ sip-bitmask <sipv6_bitmask> ]
| any } ] [ hop-limit { <hop_limit> | any } ] | ipv6-icmp [ sip { <sipv6_icmp> [ sip-
bitmask <sipv6_bitmask_icmp> ] | any } ] [ icmp-type { <icmpv6_type> | any } ] [ icmp-code
{ <icmpv6_code> | any } ] [ hop-limit { <hop_limit_icmp> | any } ] | ipv6-udp [ sip
{ <sipv6_udp> [ sip-bitmask <sipv6_bitmask_udp> ] | any } ] [ sport { <sportv6_udp_start>
[ to <sportv6_udp_end> ] | any } ] [ dport { <dportv6_udp_start> [ to <dportv6_udp_end> ] |
any } ] [ hop-limit { <hop_limit_udp> | any } ] | ipv6-tcp [ sip { <sipv6_tcp> [ sip-bitmask
<sipv6_bitmask_tcp> ] | any } ] [ sport { <sportv6_tcp_start> [ to <sportv6_tcp_end> ]
| any } ] [ dport { <dportv6_tcp_start> [ to <dportv6_tcp_end> ] | any } ] [ hop-limit
{ <hop_limit_tcp> | any } ] [ tcp-flag [ tcp-fin { <tcpv6_flag_fin> | any } ] [ tcp-
syn { <tcpv6_flag_syn> | any } ] [ tcp-rst { <tcpv6_flag_rst> | any } ] [ tcp-psh
{ <tcpv6_flag_psh> | any } ] [ tcp-ack { <tcpv6_flag_ack> | any } ] [ tcp-urg { <
tcpv6_flag_urg> | any } ] ] } ] [ action { permit | deny | filter { switchport
<filter_switch_port_list> | interface <port_type> [ <fliter_port_list> ] } } ] [ rate-
limiter { <rate_limiter_id> | disable } ] [ mirror [ disable ] ] [ logging [ disable ] ]
[ shutdown [ disable ] ] [ lookup-second [ disable ] ] [ redirect { switchport { <1-53> |
<redirect_switch_port_list> } | interface { <port_type> <redirect_port_id> | <port_type>
[ <redirect_port_list> ] } | disable } ]
```

	Argument	Description
Parameter	<ace_id>	ACE ID. The allowed range is 1–128.
	<ace_id_next>	The next ACE ID. Insert the current ACE before the next ACE ID
	<ingress_port_id>	Select the ingress port for which this ACE applies. All: The ACE applies to all ports. Port n: The ACE applies to this port number, where n is the number of the switch port.
	<ingress_port_list>	List of Port ID. For example, 1/1, 3–5; 2/2–4, 6
	<policy>	A specific policy value. The allowed range is 0–6.
	<policy_bitmask>	The Value of Policy bitmask specified in decimal or hexadecimal. The allowed range is 0x0–0x3f.
	<vid>	The value of VID field. The allowed range is 1–4095.
	<tag_priority>	The tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0–7 or range 0–1, 2–3, 4–5, 6–7, 0–3 and 4–7. The value Any means that no tag priority is specified (tag priority is **don't-care**).
	<etype_value>	The value of EtherType field. The allowed range is 0x600–0xFFFF but excluding 0x800 (IPv4), 0x806 (ARP), and 0x86DD (IPv6). The value Any means that EtherType filter is not specified (EtherType filter status is **don't-care**).
	<etype_smac>	The value of source MAC address field.
	<etype_dmac>	The value of destination MAC address field.
	<arp_sip>	The value of source IP address field.
	<arp_dip>	The value of destination IP address field.
	<arp_smac>	The value of source MAC address field.
	<arp_flag_request>	The value of ARP Request/Reply opcode field.
	<arp_flag_smac>	The value of ARP Sender Hardware Address (SHA) field.
	<arp_flag_tmac>	The value of ARP Target Hardware Address (THA) field.

.....continued

	Argument	Description
	<arp_flag_len>	The value of ARP/RARP hardware address length (HLN) and protocol address length (PLN) field.
	<arp_flag_ip>	The value of ARP/RARP hardware address space (HRD) field.
	<arp_flag_ether>	The value of ARP/RARP protocol address space (PRO) field.
	<sipv4>	The value of source IP address field.
	<dipv4>	The value of destination IP address field.
	<ipv4_protocol>	The value of IPv4 protocol field.
	<ip_flag_ttl>	The value of IPv4 TTL field.
	<ip_flag_options>	The value of IPv4 options field.
	<ip_flag_fragment>	The value of IPv4 fragment field.
	<sipv4_icmp>	The value of source IP address field.
	<dipv4_icmp>	The value of destination IP address field.
	<icmpv4_type>	The value of ICMP type field. The allowed range is 0–255.
	<icmpv4_code>	The value of ICMP code field.
	<ip_flag_icmp_ttl>	The value of IPv4 TTL field.
	<ip_flag_icmp_options>	The value of IPv4 options field.
	<ip_flag_icmp_fragment>	The value of IPv4 fragment field.
	<sipv4_udp> <sipv4_tcp>	The value of source IP address field.
	<dipv4_udp> <dipv4_tcp>	The value of destination IP address field.
	<sportv4_udp_start> <sportv4_tcp_start>	The value of UDP/TCP source port field. The allowed range is 0–65535.
	<sportv4_udp_end> <sportv4_tcp_end>	The value of UDP/TCP source port field. The allowed range is 0–65535.
	<dportv4_udp_start> <dportv4_tcp_start>	The value of UDP/TCP destination port field. The allowed range is 0–65535.
	<dportv4_udp_end> <dportv4_tcp_end>	The value of UDP/TCP destination port field. The allowed range is 0–65535.
	<ip_flag_udp_ttl> <ip_flag_tcp_ttl>	The value of IPv4 TTL field.
	<ip_flag_udp_options> <ip_flag_tcp_options>	The value of IPv4 options field.
	<ip_flag_udp_fragment> <ip_flag_tcp_fragment>	The value of IPv4 fragment field
	<tcpv4_flag_fin> <tcpv6_flag_fin>	Specify the TCP No more data from sender (FIN) value for this ACE. 0: TCP frames, where the FIN field is set, must not be able to match this entry. 1: TCP frames, where the FIN field is set, must be able to match this entry. Any: Any value is allowed (**don't-care**).
	<tcpv4_flag_syn> <tcpv6_flag_syn>	Specify the TCP Synchronize Sequence Numbers (SYN) value for this ACE. 0: TCP frames, where the SYN field is set, must not be able to match this entry. 1: TCP frames where the SYN field is set must be able to match this entry. Any: Any value is allowed (**don't-care**).

.....continued

	Argument	Description
	<tcpv4_flag_rst> <tcpv6_flag_rst>	Specify the TCP Reset the connection (RST) value for this ACE. 0: TCP frames, where the RST field is set, must not be able to match this entry. 1: TCP frames where the RST field is set must be able to match this entry. Any: Any value is allowed (**don't-care**).
	<tcpv4_flag_psh> <tcpv6_flag_psh>	Specify the TCP Push Function (PSH) value for this ACE. 0: TCP frames where the PSH field is set must not be able to match this entry. 1: TCP frames, where the PSH field is set must, be able to match this entry. Any: Any value is allowed (**don't-care**).
	<tcpv4_flag_ack> <tcpv6_flag_ack>	Specify the TCP Acknowledgment field significant (ACK) value for this ACE. 0: TCP frames, where the ACK field is set, must not be able to match this entry. 1: TCP frames where the ACK field is set must be able to match this entry. Any: Any value is allowed (**don't-care**).
	<tcpv4_flag_urg> < tcpv6_flag_urg>	Specify the TCP Urgent pointer field significant (URG) value for this ACE. 0: TCP frames, where the URG field is set, must not be able to match this entry. 1: TCP frames where the URG field is set must be able to match this entry. Any: Any value is allowed (**don't-care**).
	<next_header>	The value of IPv6 hop limiter field.
	<sipv6>	The value of source IP address field.
	<sipv6_bitmask>	The value of IPv6 source address bitmask.
	<hop_limit>	The value of IPv6 hop limiter field. Zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. Non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry. Any: Any value is allowed (**don't-care**).
	<sipv6_icmp>	The value of source IP address field.
	<sipv6_bitmask_icmp>	The value of IPv6 source address bitmask.
	<icmpv6_type>	The value of ICMP type field. The allowed range is 0–255.
	<icmpv6_code>	ICMP code value. The allowed range is 0–255.
	<hop_limit_icmp>	Hop limit settings for this ACE. Zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. Non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry. Any: Any value is allowed (**don't-care**).
	<sipv6_udp> <sipv6_tcp>	The value of source IP address field.
	<sipv6_bitmask_udp> <sipv6_bitmask_tcp>	Specific SIPv6 mask. The field only supports last 32 bits for IPv6 address.
	<sportv6_udp_start> <sportv6_tcp_start>	The value of TCP/UDP source port field start.
	<sportv6_udp_end> <sportv6_tcp_end>	The value of TCP/UDP source port field end.

.....continued		
	Argument	**Description**
	<dportv6_udp_start> <dportv6_tcp_start>	The value of TCP/UDP destination port field start.
	<dportv6_udp_end> <dportv6_tcp_end>	The value of TCP/UDP destination port field end.
	<hop_limit_udp> <hop_limit_tcp>	The value of IPv6 hop limiter field. Zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. Non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry. Any: Any value is allowed (**don't-care**).
	<filter_switch_port_list>	List of switchport ID.
	<fliter_port_list>	List of Port ID. For example, 1/1, 3–5; 2/2–4, 6.
	<rate_limiter_id>	Rate limiter ID.
	<redirect_switch_port_list>	List of switchport ID.
	<redirect_port_id>	Port ID in the format of switch-no/port-no.
	<redirect_port_list>	List of Port ID. For example, 1/1, 3–5; 2/2–4, 6.
Default	NA	
Mode	Global Configuration mode	
Usage	Set the port ACE parameters.	
Example	Set the access-list ace ID 1. `(config)# access-list ace 1`	

3.9.15 IP/IPv6 Source Guard and Port Mode Configuration

Description

Use this command to enable or disable the Global IP/IPv6 Source Guard. All configured ACEs are lost when the mode is enabled. Translate all dynamic entries to static. Specify that IP/IPv6 Source Guard is enabled on which ports and the maximum number of dynamic clients that can be learned on a given port.

```
ip verify source
```

```
ipv6 verify source
```

```
ip verify source translate
```

```
ipv6 verify source translate
```

```
ip verify source limit <cnt_var>
```

```
ipv6 verify source limit <max_dynamic_clients>
```

	Argument	**Description**
Parameter	<cnt_var>	Maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, and 2 or unlimited (for unlimited use the no version of the command).

.....continued		
	Argument	**Description**
	<max_dynamic_clients>	Maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, and 2 or unlimited (for unlimited use the no version of the command).
Default	NA	
Mode	Global Configuration mode and Port List Interface mode.	
Usage	Enable IP Source Guard. Use the no version of the command to disable IP Source Guard.	
Example	1. Enable IP Source Guard) (config)# ip verify source 2. Enable IPv6 Source Guard on port 1 and set the max number of Dynamic Clients to 2. (config)# interface GigabitEthernet 1/1 (config-if)# ipv6 verify source (config-if)# ipv6 verify source limit 2	

3.9.16 Static IP/IPv6 Source Guard Configuration

Description

Use this command to manually add a Static IP/IPv6 Source Guard entry on the given port.

```
ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>
```

```
ipv6 source binding interface <port_type> <port_type_id> [ vlan <vlan_id> ] <ipv6_ucast>
<mac_ucast>
```

	Argument	**Description**
Parameter	<port_type>	Port type in Giga or 2.5 Giga Ethernet.
	<in_port_type_id>	Port ID in the format of switch-no/port-no.
	<vlan_var> <vlan_id>	The VLAN ID for the settings.
	<ipv4_var> <ipv6_ucast>	Allowed Source IP address.
	<mac_var> <mac_ucast>	Allowed Source MAC address.
Default	NA	
Mode	Global Configuration mode.	
Usage	Add a static IP Source Guard. Use the no version of the command to delete it.	
Example	1. Add a Static IP Source Guard on port 3 with VLAN 2 IP 192.168.0.40 and MAC 10-10-10-10-10-10. (config)# ip source binding interface GigabitEthernet 1/3 2 192.168.0.40 10-10-10-10-10-10 2. Delete a Static IP Source Guard on port 3 with VLAN 2 IP 192.168.0.40 and MAC 10-10-10-10-10-10. (config)# no ip source binding interface GigabitEthernet 1/3 2 192.168.0.40 10-10-10-10-10-10	

3.9.17 ARP Inspection and Port Mode Configuration

Description
Use this command to globally enable/disable ARP Inspection and specify on which port it is enabled. Enable/Disable check VLAN operation and specify one of the three log types (Log All entries, Permitted entries, or Denied entries). Translate all dynamic entries to static entries.

```
ip arp inspection
```

```
ip arp inspection check-vlan
```

```
ip arp inspection logging { deny | permit | all }
```

```
ip arp inspection translate
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	Global Configuration and Port List Interface modes.	
Usage	Enable ARP inspection. Use the `no` version of the command to disable it.	

Example	1. Enable ARP Inspection.
	`(config)# ip arp inspection`
	2. Enable ARP inspection VLAN mode on port 1.
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# ip arp inspection check-vlan`	

3.9.18 ARP Inspection VLAN Mode Configuration

Description
Use this command to specifiy the ARP Inspection is enabled, on which VLANs it is enabled, and configure log type as per the VLAN setting.

```
ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }
```

	Argument	Description
Parameter	`<in_vlan_list>`	`ARP inspection VLAN list`
Default	NA	
Mode	Global Configuration mode	
Usage	Enable ARP inspection on VLAN. Use the `no` version of the command to Disable it.	

Example	1. Enable ARP Inspection on VLAN 5 and Log permitted entries.
	`(config)# ip arp inspection vlan 5`
	`(config)# ip arp inspection vlan 5 logging permit`
	2. Disable ARP inspection on VLAN 5
	`(config)# no ip arp inspection vlan 5`	

3.9.19 Static ARP Inspection Table Configuration

Description
Use this command to manually add a new entry to the Static ARP Inspection table on the given port.

```
ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var>
<ipv4_var>
```

	Argument	Description
Parameter	<port_type>	Port type in Giga or 2.5 Giga Ethernet.
	<in_port_type_id>	Port ID in the format of switch-no/port-no.
	<vlan_var>	The VLAN ID for the settings.
	<mac_var>	Allowed Source MAC address.
	<ipv4_var>	Allowed Source IP address.
Default	NA	
Mode	Global Configuration mode	
Usage	Add a static ARP Inspection entry. Use the no version of the command to delete it.	

Example	1. Add a Static ARP Inspection on port 3 with VLAN 2 MAC 10-10-10-10-10-10 and IP 192.168.0.40).
	`(config)# ip arp inspection entry interface GigabitEthernet 1/3 2 10-10-10-10-10-10 192.168.0.40`
	2. Delete a Static ARP Inspection on port 3 with VLAN 2 MAC 10-10-10-10-10-10 and IP 192.168.0.40).
	`(config)# no ip arp inspection entry interface GigabitEthernet 1/3 2 10-10-10-10-10-10 192.168.0.40`	

3.9.20 RADIUS Server Configuration

Description
Use this command to set default values to be used for every new RADIUS server being added when the same parameters are left blank.

```
radius-server timeout <seconds>
```

```
radius-server retransmit <retries>
```

```
radius-server deadtime <minutes>
```

```
radius-server key { [ unencrypted ] <unencrypted_key> | encrypted <encrypted_key> }
```

```
radius-server attribute 4 <ipv4>
```

```
radius-server attribute 95 <ipv6>
```

```
radius-server attribute 32 <id>
```

	Argument	Description
Parameter	<seconds>	Time to wait for a RADIUS server to reply in seconds 1–1000 before retransmitting the request. Default 5.

.....continued		
	Argument	**Description**
	<retries>	Number of times 1–1000, a request is retransmitted to a server that is not responding. Default 3.
	<minutes>	Period between 0–1440 minutes during which the switch does not send a new request to a server that failed to respond to previous requests (dead). Default 0.
	<unencrypted_key> <encrypted_key>	Specify the unencrypted or encrypted key up to 63 characters long.
	<ipv4>	IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, then the IP address of the outgoing interface is used.
	<ipv6>	IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, then the IP address of the outgoing interface is used.
	<id>	The identifier, up to 253 characters long, is used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, then the NAS-Identifier is not included in the packet.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure default global parameters for RADIUS Server. Use the no version of the command to revert to defaults.	
Example	# configure terminal (config)# radius-server timeout 10 (config)# radius-server retransmit 3 (config)# radius-server deadtime 10 (config)# radius-server key unencrypted secret	

Description
Use this command to add a new RADIUS server. Up to 5 servers can be added.

```
radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ] [ timeout
<seconds> ] [ retransmit <retries> ] [ key { [ unencrypted ] <unencrypted_key> | encrypted
<encrypted_key> } ]
```

	Argument	**Description**
Parameter	<host_name>	IPv4/IPv6 address or the hostname of the radius server.
	<auth_port>	UDP port number to use on the RADIUS server for authentication. Set to 0 to disable authentication.
	<acct_port>	UDP port number to use on the RADIUS server for accounting. Set to 0 to disable accounting.
	timeout <seconds>	Time to wait for this RADIUS server to reply (overrides default).
	retransmit <retries>	Specify the number of retries to active server (overrides default).
	<unencrypted_key> <encrypted_key>	The Unencrypted (Plain Text) or Encrypted secret key.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure custom parameters for RADIUS Server. Use the no version of the command to delete the server entry.	

.....continued		
	Argument	**Description**
Example	`# configure terminal` `(config)# radius-server host radiusserver auth-port 1812 timeout 20 retransmit 5`	

3.9.21 TACACS+ Server Configuration

Description
Use this command to set default values to be used for every new TACACS+ server being added when the same parameters are left blank.

```
tacacs-server timeout <seconds>
```

```
tacacs-server deadtime <minutes>
```

```
tacacs-server key { [ unencrypted ] <unencrypted_key> | encrypted <encrypted_key> }
```

	Argument	**Description**
Parameter	`<seconds>`	Time to wait for a TACACS+ server to reply in seconds 1—1000 before retransmitting the request. Default is 5.
	`<minutes>`	Period between 0–1440 minutes during which the switch does not send a new request to a server that failed to respond to previous requests (dead). Default is 0.
	`<unencrypted_key>` `<encrypted_key>`	The Unencrypted (Plain Text) or Encrypted secret key up to 63 characters long.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure default global parameters for TACACS server. Use the `no` version of the command to revert to default.	

Example	`# configure terminal`
	`(config)# tacacs-server timeout 10`
	`(config)# tacacs-server deadtime 3`
	`(config)# tacacs-server key unencrypted secret`	

Description
Use this command to add a new TACACS+ server. Up to 5 servers can be added.

```
tacacs-server host <host_name> [ port <port> ] [ timeout <seconds> ] [ key { [ unencrypted ]
<unencrypted_key> | encrypted <encrypted_key> } ]
```

	Argument	**Description**
Parameter	`<host_name>`	IPv4/IPv6 address or the hostname of the radius server
	`<port>`	TCP port number to use on the TACACS+ server for authentication.
	`timeout <seconds>`	Time to wait for this TACACS+ server to reply (overrides default).
	`<unencrypted_key>`	The UNENCRYPTED (Plain Text) secret key (overrides default)
Default	NA	

.....continued		
	Argument	**Description**
Mode	Global Configuration mode	
Usage	Configure custom parameters for TACACS+ Server. Use the `no` version of the command to delete the server enty.	
Example	`# configure terminal` `(config)# tacacs-server host tacacsserver port 50 timeout 20 key unencrypted secret`	

3.10 Aggregation Configuration

Use this command to employ multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

3.10.1 Common Aggregation Configuration

Description
Use this command to configure the Aggregation hash mode. This mode applies to the whole network element.

```
aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }
```

	Argument	**Description**
Parameter	`[ smac ]`	Source MAC address can be used to calculate the destination port for the frame (enabled by default).
	`[ dmac ]`	Destination MAC address can be used to calculate the destination port for the frame (disabled by default).
	`[ ip ]`	IP address can be used to calculate the destination port for the frame (enabled by default).
	`[ port ]`	TCP/UDP port number can be used to calculate the destination port for the frame (enabled by default).
Default	smac, ip, and port enabled. dmac disabled.	
Mode	Global Configuration mode	
Usage	Configure aggregation parameters. Use the `no` version of the command to reset to default.	

Example	Enable smac and dmac only
	`# configure terminal`
	`(config)# aggregation mode smac dmac`	

3.10.2 Aggregation Group Configuration

Description
Use this command to create and configure aggregation group. Each port can be a member of one aggregation group only and ports must be full duplex and have the same speed. Also, it specifies the Aggregation mode.

```
aggregation group <v_uint> mode { [ active | on | passive ] }
```

	Argument	**Description**
Parameter	`<v_uint>`	The aggregation group id 1–3.
	`[ active ]`	Group operates in LACP active aggregation mode.
	`[ on ]`	Group operates in a static aggregation mode.

.....continued		
	Argument	**Description**
	`[ passive ]`	Group operates in LACP passive aggregation mode.
Default	NA	
Mode	Port List Interface mode	
Usage	Configure aggregation group (add port to it). Use the `no` version of the command to remove the port from the aggregation group.	

Example	Configure port 1 to be a member of aggregation group 1 operation in active LACP mode.
	`# configure terminal`
	`(config)# interface GigabiitEthernet 1/1`
	`(config-if)# aggregation group 1 mode active`	

3.10.3 LACP System Configuration

Description
Use this command to specify if the group performs automatic link (re-) calculation, when links with higher priority become available (revertive) and the maximum number of active bundled LACP ports allowed in an aggregation. It also sets the LACP timeout on the port, that is, how fast to transmit BPDUs, once a second (fast) or once each 30 seconds (slow) and priority.

```
lacp failover { revertive | non-revertive }
```

```
lacp max-bundle <v_uint>
```

```
lacp timeout { fast | slow }
```

```
lacp port-priority <v_1_to_65535>
```

```
lacp system-priority <v_1_to_65535>
```

	Argument	**Description**
Parameter	`revertive`	Group performs automatic link recalculation.
	`non-revertive`	Group does not perform automatic link recalculation.
	`<v_uint>`	This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.
	`<v_1_to_65535>`	Priority value 1 to 65535. Lower means higher priority.
Default	Revertive failover is enabled.	
Mode	LLAG and Port List Interface modes	
Usage	Specifies if the group will perform automatic link recalculation. Use the `no` version of the command to revert to default.	

Example	Set failover to non-revertive on interface LLAG 1 with maximum bundle 4.
	`# configure terminal`
	`(config)# interface llag 1`
	`(config-llag)# lacp failover non-revertive`
	`(config-llag)# lacp max-bundle 4`	

3.11 Loop Protection Configuration

Loop protect feature can prevent Layer2 loops by sending the loop protect protocol packets and shutting down interfaces if they receive loop protect packets that have originated from themselves.

3.11.1 Loop Protection General Settings

Description
Configure Loop protection general parameters.

```
loop-protect
```

```
loop-protect transmit-time <t>
```

```
loop-protect shutdown-time <t>
```

	Argument	Description
Parameter	`transmit-time <t>`	Interval between each loop protection PDU sent on each port. Valid values are 1–10 seconds. Default is 5.
	`shutdown-time <t>`	Period for which the port is kept disabled if a loop is detected. Valid values 0–604800 seconds (7 days). A value of 0 keeps the port disabled until the next device restart. Default is 180.
Default	NA	
Mode	Global Configuration mode	
Usage	Enable/Disable Loop protection (globally) and configure Loop protection parameters. Use the `no` version of the command to reset to default.	

Example	Enable Loop protection and set transmit time to 8 seconds, shutdown time to 500 seconds.
	`# configure terminal`
	`(config)# loop-protect`
	`(config)# loop-protect transmit-time 8`
	`(config)# loop-protect shutdown-time 500`	

3.11.2 Loop Protection General Settings

Description
Configures Loop protection parameters for the switch port.

```
loop-protect
```

```
loop-protect action { [ shutdown ] [ log ] }
```

```
loop-protect tx-mode
```

	Argument	Description
Parameter	`shutdown`	Shutdown the port when the Loop is detected.
	`log`	Log only when the Loop is detected.
	`tx-mode`	Controls if the port is actively generating loop protection PDUs or if it is passively looking for looped PDUs.

.....continued		
	Argument	**Description**
Default	NA	
Mode	Port List Interface mode	
Usage	Enable/Disable Loop protection on a switch port and configure Loop protection parameters.	

Example	Enable Loop protection on port 1, set it to Shutdown and Log when the loop is detected, and disable the Tx mode.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# loop-protect`
	`(config-if)# loop-protect action shutdown log`
	`(config-if)# no loop-protect tx-mode`	

3.12 Spanning Tree Configuration

Spanning Tree Protocol (STP) and its variations as RSTP and MSTP are used to prevent possible Network loops, which without STP, might cause broadcast storming. It also offers redundancy path from switch to switch or path to path over multiple switches by supporting Network loops under the control of STP.

3.12.1 STP Bridge Configuration

Description
Use this command to configure the STP protocol version, bridge priority, the interval between sending STP BPDUs, the delay used by STP Bridges to transit Root and Designated Ports to Forwarding, the maximum age of the information transmitted by the Bridge when it is the Root Bridge, hop count range, and maximum number of transmit BPDUs per second.

Following are the basic STP Global Setting commands.

```
spanning-tree mode { stp | rstp | mstp }
```

```
spanning-tree mst <instance> priority <prio>
```

```
spanning-tree mst hello-time <hellotime>
```

```
spanning-tree mst forward-time <fwdtime>
```

```
spanning-tree mst max-age <maxage> [ forward-time <fwdtime> ]
```

```
spanning-tree mst max-hops <max_hops>
```

```
spanning-tree transmit hold-count <holdcount>
```

Following are the Advanced STP Global Setting commands.

```
spanning-tree edge bpdu-filter
```

```
spanning-tree edge bpdu-guard
```

```
spanning-tree recovery interval <interval>
```

	Argument	Description
Parameter	<instance>	STP bridge instance. Must be 0 (zero) for CIST.
	priority <prio>	Bridge Priority. Supported values are 0–61440. Only values divisible by 4096 are allowed. For example, 4096, 8192, and so on. Default value is 32768.
	<hellotime>	Interval between sending STP BPDUs. Valid values are 1–10 seconds. Default is 2 seconds.
	<fwdtime>	Forward delay used by STP Bridges to transit Root and Designated Ports to Forwarding. Valid values are 4–30 seconds. Default is 15.
	<maxage>	Maximum age of the information transmitted by the Bridge when it is a Root Bridge. Valid values are 6–40 seconds. Default is 20.
	<maxhops>	Defines how many bridges a root bridge can distribute its BPDU information. Valid values are 6-–40 hops. Default is 20.
	<holdcount>	Number of BPDUs a bridge port can send per second. Valid range 1–10 BPDUs per second. Default is 6.
	<interval>	Time to pass before a port in error-disabled state can be enabled. Values are 30–86400 seconds (24 hours). Default is port error recovery disabled.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure STP system settings. Use the no version of the command to revert to default.	
Example	Configure STP settings # configure terminal (config)# spanning-tree mode mstp (config)# spanning-tree mst 0 priority 36864 (config)# spanning-tree mst hello-time 3 (config)# spanning-tree mst max-age 25 forward-time 16 (config)# spanning-tree mst max-hops 25 (config)# spanning-tree transmit hold-count 7 (config)# spanning-tree edge bpdu-filter (config)# spanning-tree edge bpdu-guard (config)# spanning-tree recovery interval 120	

3.12.2 MSTI Mapping Configuration

Description
Use this command to configure STP MSTI bridge instance priority name and revision. Add VLANs. Unmapped VLANs are mapped to the CIST (the default bridge instance). The Traffic Engineering (TE) instance is special, as it is not controlled by MSTP itself. The TE instance is always forwarding for all ports.

```
spanning-tree mst name <name> revision <v_0_to_65535>
```

```
spanning-tree mst <instance> vlan <v_vlan_list>
```

```
spanning-tree mst te vlan <v_vlan_list>
```

	Argument	Description
Parameter	<name>	The name identifying the VLAN to MSTI mapping. The name is at most 32 characters.
	<v_0_to_65535>	The revision of the MSTI configuration. This must be an integer between 0 and 65535.
	<instance>	STP bridge instance. MSTI1 = 1, MSTI2 = 2 to MSTI7 = 7.
	<v_vlan_list>	The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN or a range (xx–yy), each of which must be separated with comma and/or space.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure MSTI settings. Use the no version of the command to revert to default.	
Example	Configure STP MSTI configuration name as 12345 with revision 1. # configure terminal (config)# spanning-tree mst name 12345 revision 1	

3.12.3 MSTI Priority Configuration

Description
Use this command to configure STP MSTI bridge instance priority.

```
spanning-tree mst <instance> priority <prio>
```

	Parameter	Description
Parameter	<instance>	STP bridge instance. Must be 0 (zero) for CIST and 1–7 for MSTI.
	priority <prio>	Bridge Priority. Supported values are 0–61440. Only values divisible by 4096 are allowed. For example, 4096, 8192, 12288, and so on. Default value is 32768.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure STP system settings. Use the no version of the command to revert to default.	
Example	Configure STP MSTI2 Priority 12288 # configure terminal (config)# spanning-tree mst 2 priority 12288	

3.12.4 CIST/MSTI Port Configuration

Description
Use this command to configure STP CIST/MSTI aggregated and normal ports parameters.

```
spanning-tree aggregation
```

```
spanning-tree mst <instance> cost { <cost> | auto }
```

```
spanning-tree mst <instance> priority <prio>
```

```
spanning-tree edge
```

```
spanning-tree auto-edge
```

```
spanning-tree restricted-role
```

```
spanning-tree restricted-tcn
```

```
spanning-tree bpdu-guard
```

```
spanning-tree link-type { point-to-point | shared | auto }
```

	Parameter	Description
Parameter	<instance>	STP bridge instance. It must be 0 (zero) for CIST and 1–7 for MSTI.
	priority <prio>	Port priority must be divisible by 16. Supported values are 0/16/32/48/64/80/96/112/128/144/160/176/192/208/224/240. Default value is 128.
	<cost>	The Auto setting sets the path cost as appropriate by the physical link speed, using the 802.1D recommended values. A user-defined value can be entered. Valid values are in the range 1 to 200000000.
Default	NA	
Mode	STP Aggregation and Port List Interface modes.	
Usage	Configure STP CIST/MSTI aggregated and normal ports parameters. Use the no version of the command to revert to default.	
Example	1. Configure CIST Aggregated port priority 32. # configure terminal (config)# spanning-tree aggregation (config-stp-aggr)# spanning-tree mst 0 port-priority 32 2. Configure CIST port 2 priority 64 with auto edge disabled. (config)# interface GigabitEthernet 1/2 (config-if)# spanning-tree mst 0 port-priority 64 (config-if)# spanning-tree no auto-edge	

3.13 LLDP Configuration

The Link Layer Discovery Protocol (LLDP) allows stations attached to LAN to advertise, to other stations attached to the same LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to LAN required by those management entity or entities.

3.13.1 LLDP Parameters Configuration

Description
Use this command to configure LLDP Interval (seconds between each LLDP frame), Hold (times the information in the LLDP frame considered valid), Delay (seconds between changed LLDP frame), and Reinit (seconds between the shutdown frame and a new LLDP initialization).

```
lldp timer <val>
```

```
lldp holdtime <val>
```

```
lldp transmission-delay <val>
```

```
lldp reinit <val>
```

	Parameter	Description
Parameter	`timer <val>`	The interval between each LLDP frame is determined. Valid values are 5–32768 seconds. Default 30 seconds.
	`holdtime <val>`	Valid values are 2–10 times. Default is 4.
	`transmission-delay <val>`	Cannot be larger than 1/4 of the interval value. Valid values are 1–8192 seconds. Default is 2.
	`reinit <val>`	Valid values are 1–10 seconds. Default is 2.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure LLDP parameters. Use the `no` version of the command to revert to default.	

Example	1. Configure LLDP interval to 20 seconds.
	`# configure terminal`
	`(config)# lldp timer 20`
	2. Revert LLDP timer to default 30 seconds.
	`(config)# no lldp timer`	

3.13.2 LLDP Interface Configuration

Description
Use this command to configure LLDP parameters for each port. Select LLDP mode, CDP awareness, configure if an SNMP trap is emitted when the LLDP neighbor table changes, and select optional TLVs (port description, system name, description, capabilities, management address) when LLDP information is transmitted.

```
lldp transmit
```

```
lldp receive
```

```
lldp cdp-aware
```

```
lldp trap
```

```
lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }
```

	Parameter	Description
Parameter	`transmit`	Enable/Disabled transmission of LLDP frames.
	`receive`	Enable/Disable decoding of received LLDP frames.
	`cdp-aware`	Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table).
	`trap`	Configures if an SNMP trap is emitted when the LLDP neighbor table changes for the interface.
	`tlv-select`	Enables/disables LLDP optional TLVs to transmit.
Default	NA	
Mode	Port List Interface mode	
Usage	Enable LLDP system settings. Use the `no` version of the command to disable.	

Example	Configure LLDP on port 1 as transmit only with CDP aware.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# no lldp recieve`
	`(config-if)# lldp cdp-aware`	

3.13.3 LLDP-MED Interface Configuration

Description
LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association. This function applies to VoIP devices which support LLDP-MED.

```
lldp med fast <v_1_to_10>
```

```
lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ] [ poe ]
```

```
lldp med type { connectivity | end-point }
```

```
lldp med location-tlv latitude { north | south } <v_word8>
```

```
lldp med location-tlv longitude { west | east } <v_word9>
```

```
lldp med location-tlv altitude { meters | floors } <v_word11>
```

```
lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }
```

```
lldp med location-tlv civic-addr { { country <country> } | { state | county | city | district
| block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-
no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment
| floor | room-number | place-type | postal-community-name | p-o-box | additional-code }
<v_line> }
```

```
lldp med location-tlv elin-addr <v_word25>
```

```
lldp med media-vlan policy-list <v_range_list>
```

```
lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling
| guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling }
{ untagged | tagged <v_vlan_id> [ l2-priority <v_0_to_7> ] } [ dscp <v_0_to_63> ]
```

	Parameter	Description
Parameter	`fast <v_1_to_10>`	Specify the number of times from 1 to 10 the fast start transmission would be repeated. Default value 4.
	`transmit-tlv`	Specify which TLVs included in LLDP-MED information transmitted.
	`type`	Specify the type of LLDP-MED Device, which may be either a Network Connectivity Device (Router, Bridge, Access Point, and so on) or a specific class of Endpoint Device.
	`{ north | south } <v_word8>`	Latitude must be normalized to within 0–90 degrees with a maximum of four digits. Specify the direction to either North or South of the equator.
	`{ west | east } <v_word9>`	Longitude must be normalized to within 0–180 degrees with a maximum of four digits. Specify the direction to either East or West of the prime meridian.
	`{ meters | floors } <v_word11>`	Altitude must be normalized to within −2097151.9 to 2097151.9 with a maximum of 1 digit. Select between two altitude types (floors or meters).

.....continued		
	Parameter	**Description**
	datum	The Map Datum is used for the coordinates given in three options. WGS84: (Geographical 3D)—World Geodesic System 1984, CRS Code 4327 NAD83/NAVD88: North American Datum 1983, CRS Code 4269 or NAD83/MLLW: North American Datum 1983, CRS Code 4269
	civic-addr <v_line>	IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.
	elin-addr <v_word25>	Emergency Call Service ELIN identifier. Consists of a numerical digit string up to 25 characters.
	policy-list <v_range_list>	Policies to assign to the interface.
	policy <policy_index>	Crate a new policy with ID 0–31. Specify application type, Tagged or Untagged VLANs, L2 priority 0–7, and DSCP 0–63.
Default	NA	
Mode	Port List Interface mode and Global Configuration mode for creating a media-vlan-policy.	
Usage	Enable LLDP parameters of the interface. Use the no version of the command to disable.	
Example	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# lldp med transmit-tlv capabilities (config-if)# lldp med transmit-tlv poe (config-if)# no lldp med transmit-tlv location (config-if)# lldp med type end-point	

3.14 Power over Ethernet Configuration

Use this command to configure the PoE system and the port parameters.

3.14.1 PoE System Configuration

Description

Use this command to configure system parameters. Interruptible power controls if PoE power should be interrupted (shut down for 5s) during unit software restart cycle (Enabled) or remain unchanged during the unit software restart cycle (Disabled). Enable/Disable PD Auto-class request (PD communicates its effective maximum power consumption to the PSE). Specify the Legacy PD-Class mode.

```
poe interruptible-power
```

```
poe pd-auto-class-request
```

```
poe legacy-pd-class-mode { standard | poh | ignore-pd-class }
```

	Parameter	Description
Parameter	`standard`	Extend PD detection resistance/capacitance range beyond IEEE® 802.3bt specification. Power-Demotion, that is, PD is allocated power from a PSE that is lower than what the PD requested, is supported.
	`poh`	Same as Standard-Mode except for PoE-AT PDs advertising class 4, 4 (DSPD) or class 4 (SSPD). PoE-AT DSPD class 4, 4 is offered 90W (instead of 60W). PoE-AT SSPD class 4 is offered 45W (instead of 30W). No support for Power-Demotion. **Note:** PoE-BT class 4,4 PD is offered 60W and PoE-BT SSPD class 4 is offered 30W.
	`ignore-pd-class`	Port configured as Type4-90W is limited to 90W (DSPD) or 45W (SSPD) regardless of PD advertised class. No support for Power-Demotion. Port configured as Type3-60W is limited to 60W (DSPD) or 30W (SSPD) regardless of PD advertised class. No support for Power-Demotion. Port configured as Type3-30W/Type3-15W performs as if it was configured in the Standard-Mode.
Default	NA	
Mode	Global Configuration mode	
Usage	Enable PoE system parameters. Use the `no` version of the command to disable.	

Example	Enables PoE interruptible power, set the PD-class mode to PoH and disable PD Auto-class.
	`# configure terminal`
	`(config)# poe interruptible-power`
	`(config)# poe legacy-pd-class-mode poh`
	`(config)# no poe pd-auto-class-request`	

3.14.2 PoE Port Configuration

Description
Use this command to configure the PoE port parameters. Set the maximum power the PoE port can deliver to the PD, PoE, and Power Management mode, PoE port priority, enable/disable LLDP on the port, and specify the cable length to assist in port power optimization.

```
poe type { type3-15w | type3-30w | type3-60w | type4-90w }
```

```
poe mode { standard | plus }
```

```
poe power-management { dynamic | static | hybrid }
```

```
poe priority { low | high | critical }
```

```
poe lldp
```

```
poe max-cable-length { max-10 | max-30 | max-60 | max-100 }
```

	Argument	Description
Parameter	`type3-15w | type3-30w | type3-60w | type4-90w`	The maximum power the PoE port can deliver to the PD before shutting it down. Power demotion is supported, and a lower power may in effect by provided. Default is 90W.

.....continued		
	Argument	**Description**
	`standard`	PoE port is enabled and compliant with IEEE® 802.3bt specification. Default setting is standard.
	`plus`	PoE port is enabled and supports non IEEE-802.3-af/at/bt PoE PDs. Default setting is standard
	`dynamic`	Deduct from the free available power the actual PD power consumption, ignoring PD class. Default setting is dynamic.
	`static`	Use PD class to deduct from the free available power, considering power demotion, while ignoring actual PD power consumption. Default setting is dynamic.
	`hybrid`	Mixture of dynamic and static power management. Any PoE port configured as Hybrid acts as if it is configured to dynamic mode unless it has negotiated a maximum power consumption over LLDP. A port that negotiated a successful maximum PoE power over LLDP is switched automatically to static mode limited to the negotiated power. Default setting is dynamic.
	`low | high | critical`	Controls the order of the PoE ports during Power-On and Power-Off sequence when overall power consumption exceeds the maximum available power. Critical ports Turn ON first and Turn OFF last. Default priority is Low.
	`max-10 | max-30 | max-60 | max-100`	Ethernet cable length. The default value is 100m.
Default	NA	
Mode	Port List Interface mode	
Usage	Configure PoE port parameters. Use the `no` version of the command to revert to default or for disable poe mode.	

Example	1. Disable PoE on port 1.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# no poe mode`
	2. Enable PoE on port 1, set the mode to plus, power to 30W, and enable LLDP.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# poe mode plus`
	`(config-if)# poe type type3-30w`
	`(config-if)# poe lldp`	

3.15 MAC Address Table Configuration

Provides various options regarding the way MAC address learning must be processed by the Ethernet Switch, and how to process a packet with unknown source MAC address, unknown destination MAC address, and so on.

When a packet is received, it is classified by its Source-MAC, Destination-MAC, VLAN-ID, and Port number. As part of the Ethernet Switch forwarding algorithm, the switch looks for Destination-MAC and VLAN inside the MAC learning table. If it was found, then the packet is forwarded to the specified port. Otherwise, the packet is flooded to all ports on the same VLAN.

3.15.1 Aging Configuration

Description
By default, the dynamic entries are removed from the Mac table after 300 seconds. This process is called aging. Aging time can be configured to be in the range of 10 to 1000000 seconds or 0 to disable automatic aging.

```
mac address-table aging-time <v_0_10_to_1000000>
```

	Argument	Description
Parameter	`<v_0_10_to_1000000>`	Aging time in seconds, 0 to disable aging.
Default	Aging time is 300 seconds	
Mode	Global Configuration mode	
Usage	Set MAC address table aging time in seconds. Use the `no` version of the command to reset to default (300 seconds)	

Example	1. (Set aging time to 400 seconds.
	`(config)# mac address-table aging-time 400`
	2. Disable automatic aging
	`(config)# mac address-table aging-time 0`	

3.15.2 MAC Table and VLAN Learning

Description
Each port can do learning in Auto mode (done automatically as soon as the frame with unknown MAC is received) or Secured mode (only static MAC entries are learned and all other frames are dropped). MAC learning can also be disabled, and no learning is done. Specific VLANs can also be learning-disabled.

```
mac address-table learning [ secure ]
```

```
mac address-table learning vlan <vlan_list>
```

	Argument	Description
Parameter	`[ secure ]`	Port Secure mode
Default	All ports are in Auto learning mode	
Mode	List Interface mode (for specific port), Global Configuration mMode (for VLANs).	
Usage	Set MAC address table learning mode to Secure or back to Auto (command without [secure] parameter). Use the `no` version of the command to Disable learning.	

Example	1. Set MAC address learning to Secure on port 1.
	`(config)#interface GigabitEthernet 1/1`
	`(config-if)#mac address-table learning secure`
	2. Disable MAC address learning on ports 2–4.
	`(config)# interface GigabitEthernet 1/2-4`
	`(config-if)#no mac address-table learning`
	3. Add VLAN2 to the list of learning disabled VLANs.
	`(config)# no mac address-table learning vlan 2`	

3.15.3 Static MAC Table Configuration

Description
Assign a static mac address to the specific port or ports

```
mac address-table static <v_mac_addr> vlan <v_vlan_id> { [ interface <port_type>
[ <v_port_type_list> ] ] }
```

	Argument	Description
Parameter	<v_mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
	<v_vlan_id>	VLAN IDs 1-4095
	<port_type>	Gigabit Ethernet
	<v_port_type_list>	List of Port ID. For example, 1/1, 3–4.
Default	NA	
Mode	Global Configuration mode	
Usage	Assigns a static MAC address to a port. Use the no version of the command to remove it.	
Example	Assign static MAC address 00:11:22:33:44:55 to port 1 on VLAN 1. (config)#mac address-table static 00:11:22:33:44:55 vlan 1 interface Gi 1/1	

3.16 VLAN Configuration

Use this command to configure global and per port VLAN parameters.

3.16.1 Global VLAN Configuration

Description
Creates one or more VLANs in the Access mode. By default, only single VLAN #1 is enabled with all ports assigned to this VLAN in the Access mode. Specify the Ethertype/TPID used for Custom S-Ports. The setting is in force for all ports set to S-Custom port type.

```
vlan <vlist>
```

```
vlan ethertype s-custom-port <etype>
```

	Argument	Description
Parameter	<vlist>	The allowed Access VLAN IDs. Individual elements are separated by commas and ranges are specified with a dash.
	<etype>	EtherType/TPID specified in hexadecimal (Range: 0x0600-0xffff)
Default	TPID is set to 0x88A8	
Mode	Global Configuration mode	
Usage	Create allowed Access VLANs. Use the no version of the command to delete VLANs and revert TPID back to default.	
Example	1. Create Access VLANs 10, 11, 12, 200, and 300. (config)# vlan 10-12,200,300 2. Delete VLAN 12. (config)# no vlan 12 3. Set TPID=8888. (config)# vlan ethertype s-custom-port 0x8888	

3.16.2 Port VLAN Configuration

Description
Use this command to define the port mode as access (default), trunk, or hybrid unconditionally.

```
switchport mode { access | trunk | hybrid }
```

	Argument	Description
Parameter	access	Configure a switch port mode is access.
	trunk	Configure a switch port mode is trunk.
	hybrid	Configure a switch port mode is hybrid.
Default	The switch port default mode is access.	
Mode	Port List Interface mode	
Usage	Set port mode. Use the no version of the command to revert to default.	
Example	Configure the port 3 mode as trunk. # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk	

Description
Use this command to configure VLAN ID to be added internally by the Switch when the native VLAN packet (packet with no VLAN header) is received.

```
switchport trunk native vlan <pvid>
```

```
switchport hybrid native vlan <pvid>
```

	Argument	Description
Parameter	<pvid>	VLAN ID of the native VLAN when this port is in trunk/ hybrid mode
Default	Trunk/Hybrid native default VLAN is VLAN1.	
Mode	Port List Interface mode	
Usage	Configure a port VLAN ID for a trunk/hybrid port. use the no version of the command to revert to default.	
Example	Configure port 3 as trunk with PVID 4. # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4	

Description
Port in Trunk mode may control the tagging of frames on egress. Options are default Untag Port VLAN (frames classified to the Port VLAN are transmitted untagged and all other frames are transmitted with the relevant tag) and Tag all (all frames transmitted with a tag).

```
switchport trunk vlan tag native
```

	Argument	Description
Parameter	NA	NA
Default	Frames classified to the Port VLAN (Native VLAN) do not get tagged on egress.	
Mode	Port List Interface mode	
Usage	Set the trunk port egress tagging to all. Use the `no` version of the command to revert to default (untag native VLAN).	

Example	Configure port 3 as trunk with PVID 4 and set egress tagging to tag all.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/3`
	`(config-if)# switchport mode trunk`
	`(config-if)# switchport trunk native vlan 4`
	`(config-if)# switchport trunk vlan tag native`	

Description

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. By default, Trunk or Hybrid port becomes a member of all VLANs (1–4095). The port can also be configured to never become a member of one or more VLANs (forbidden VLANs).

```
switchport trunk allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
```

```
switchport forbidden vlan { add | remove } <vlan_list>
```

	Argument	Description
Parameter	`all`	All VLANs are allowed (1–4095).
	`none`	Port does not become member of any VLAN
	`add`	Add VLANs to the current list.
	`remove`	Remove VLANs from the current list.
	`except`	All VLANs except the following (VLAN ID or list).
	`<vlan_list>`	VLAN IDs. Individual elements are separated by commas and ranges are specified with a dash.
Default	All VLANs are allowed (1–4095).	
Mode	Port List Interface mode	
Usage	Configure allowed/forbidden VLANs for a port. Use the `no` version of the command to revert to default.	

Example	1. Configure port 3 as trunk and exclude VLAN 10 and 30,31,32 from allowed VLANs.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/3`
	`(config-if)# switchport mode trunk`
	`(config-if)# switchport trunk allowed vlan except 10,30-32`
	2. Configure port 3 as trunk and add VLAN 4 to the list of forbidden VLANs.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/3`
	`(config-if)# switchport mode trunk`
	`(config-if)# switchport forbidden vlan add 4`	

Description
Use this command to specify the port type in hybrid mode.

```
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
```

	Argument	Description
Parameter	`unaware`	Port is not aware of VLAN tags. No matter the received frame is tagged or untagged, port adds a tag (based on PVID) to the frame and then forward it.
	`c-port`	Customer port. If the received frame is untagged, C-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it is forwarded without adding a tag.
	`s-port`	Provider port. Port only accepts untagged frames. If the received frame is untagged, S-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it is discarded.
	`s-custom-port`	Custom provider port. When Ethertype is set to 0x8100, S-custom ports do the same as C-ports: If the received frame is untagged, S-custom port adds a tag (based on PVID) to the frame and then forwards it. If the frame is already tagged, it is forwarded without adding a tag.
Default	Hybrid Port type is C-port	
Mode	Port List Interface mode	
Usage	Configure hybrid port type. Use the no version of the command to revert to default.	

Example	Configure port 3 as hybrid Unaware type.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/3`
	`(config-if)# switchport mode hybrid`
	`(config-if)# switchport hybrid port-type unaware`	

Description
Use this command to enable or disable ingress filtering on hybrid ports. Access and Trunk ports always have ingress filtering enabled. Set Ingress acceptance criteria.

```
switchport hybrid ingress-filtering
```

```
switchport hybrid acceptable-frame-type { all | tagged | untagged }
```

	Argument	Description
Parameter	`all`	Both tagged and untagged frames are accepted
	`tagged`	Only frames tagged with the corresponding port type tag are accepted.
	`untagged`	Only untagged frames are accepted.
Default	Ingress filtering disabled. Hybrid Port is set to accept all frames (tagged and untagged).	
Mode	Port List Interface mode	
Usage	Enable ingress filtering and configure type of frames accepted on ingress. Use the `no` version of the command to revert to default.	

.....continued		
	Argument	**Description**

Example	Configure port 3 as hybrid, enable ingress filtering, and accept tagged frames only on ingress.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/3`
	`(config-if)# switchport mode hybrid`
	`(config-if)# switchport hybrid ingress-filtering`
	`(config-if)# switchport hybrid acceptable-frame-type tagged`	

Description
Use this command to configure Egress tagging on hybrid port.

```
switchport hybrid egress-tag { none | all [ except-native ] }
```

	Argument	**Description**
Parameter	`none`	No Egress tagging. All frames transmitted without a tag.
	`all`	Tag all frames. All frames are transmitted with a tag.
	`except-native`	Tag all frames except frames classified to native VLAN.
Default	Hybrid port is set to tag all frames except frames classified to native VLAN.	
Mode	Port List Interface mode	
Usage	Configure egress tagging. Use the `no` version of the command to revert to default.	

Example	Configure port 3 as hybrid and set egress tagging to all.
	`# configure terminal`
	`(config)# interface GigabitEthernet 1/3`
	`(config-if)# switchport mode hybrid`
	`(config-if)# switchport hybrid egress-tag all`	

3.16.3 Shared VLAN Learning Configuration

Description
Shared VLAN Learning allows for frames initially classified to a particular VLAN (based on Port VLAN ID or VLAN tag information) be bridged on a shared VLAN. In SVL, two or more VLANs are grouped to share the common source address information in the MAC table. The common entry in the MAC table is identified by a Filter ID (FID).

```
svl fid <fid> vlan <vlan_list>
```

```
no svl fid { <fid_list> | all }
```

	Argument	**Description**
Parameter	`<fid>`	The Filter ID (FID). must be a number between 1 and 63.
	`<vlan_list>`	List of VLANs mapped into FID. Individual elements are separated by commas and ranges are specified with a dash.
	`<fid_list> | all`	List of one, more, or all Filter IDs (FIDs).
Default	NA	

.....continued		
	Argument	**Description**
Mode	Global Configuration mode	
Usage	Create Shared VLAN Learning (SVL). Use the `no` version of the command to change all VIDs currently mapped to the FID back to being independent (IVL).	

Example	1. Let VID 2, 4, and 20-200 map to the same shared VLAN, 13.
	`(config)# svl fid 13 vlan 2,4,20-200`
	2. Let all VLANs currently mapped to FID 7 and 10 return to Independent VLAN Learning (IVL).
	`(config)# no svl fid 7,10`	

3.17 QoS Configuration

Quality of Service (QoS) is a method to guarantee a bandwidth relationship between individual applications or protocols.

3.17.1 QoS Port Classification Configuration

Description

Use this command to configure the basic QoS Classification settings for all switch ports. Select Class of Service (CoS), Drop Precedence Level (DPL), Priority Code Point (PCP) and, Drop Eligible Indicator (DEI) values. This command enables/disables DSCP Based QoS Ingress port classification and specifies QoS Control Entry (QCE) combinations of keys and actions.

```
qos cos <cos>
```

```
qos dpl <dpl>
```

```
qos pcp <pcp>
```

```
qos dei <dei>
```

```
qos trust dscp
```

```
qos qce { [ addr { source | destination } ] [ key { double-tag | normal | ip-addr | mac-ip-addr } ] }
```

	Argument	**Description**
Parameter	`<cos>`	Class of Service value 0–7. Default is 0.
	`<dpl>`	Drop Precedence Level value 0–1. Default is 0.
	`<pcp>`	Priority Code Point value 0–7. Default is 0.
	`<dei>`	Drop Eligible Indicator value 0–1. Default is 0.
	`{ source | destination }`	Specify whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on the port.
	`double-tag`	Quarter key, match inner and outer tag.
	`normal`	Half key, match outer tag, SIP/DIP, and SMAC/DMAC.
	`ip-addr`	Half key, match inner and outer tag, SIP, and DIP. For non-IP frames, match outer tag only.
	`mac-ip-addr`	Full key, match inner and outer tag, SMAC, DMAC, SIP, and DIP.
Default	NA	

.....continued		
	Argument	**Description**
Mode	Port List Interface mode	
Usage	Configure basic QoS settings. Use the `no` version of the command to revert to default.	

Example	Set the QoS DPL to 1 and enable DSCP on port 1.
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# qos dpl 1`
	`(config-if)# qos trust dscp`	

3.17.2 QoS Port Policing Configuration

Description
Use this command to configure the Port Policer settings for all switch ports. A Policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

```
qos policer <rate> [ kbps | mbps | fps | kfps ] [ flowcontrol ]
```

	Argument	**Description**
Parameter	`<rate>`	The rate for the port policer. This value is restricted to 100–3276700 when the unit is kbps or fps, and 1–3276 when unit is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.
	`flowcontrol`	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.
Default	Disabled.	
Mode	Port List Interface mode	
Usage	Configure the policer rate and enable flow control. Use the `no` version of the command to revert to default.	

Example	Set policer to 200 Mbps with flow control enabled on port 1.
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# qos dpl 1`
	`(config-if)# qos trust dscp`	

3.17.3 QoS Queue Policing Configuration

Description
Use this command to enable or disable the Queue Policer settings for all switch ports.

```
qos queue-policer queue <queue> <rate> [ kbps | mbps ]
```

	Argument	**Description**
Parameter	`<queue>`	Specific queue or range 0–7.
	`<rate>`	Controls the rate for the queue policer. This value is restricted to 100–3276700 when the unit is kbps, and 1–3276 when the unit is Mbps. The rate is internally rounded up to the nearest value supported by the queue police.
Default	NA	

.....continued		
	Argument	**Description**
Mode	Port List Interface mode	
Usage	Enable the queue policer for this switch port. Use the `no` version of the command to disable.	

Example	Enable Queue Policer 0 for port 1 with rate 100 mbps.
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# qos queue-policer queue 0 100 mbps`	

3.17.4 QoS Egress Port Scheduler and Shapers Configuration

Description
Use this command to configure the Scheduler and Shapers for a specific port. The Scheduler Mode Weighted Round Robin (WRR) controls how many queues are scheduled as strict and how many are scheduled as weighted on this switch port.

```
qos wrr <w0> <w1> [ <w2> [ <w3> [ <w4> [ <w5> [ <w6> [ <w7> ] ] ] ] ] ]
```

```
qos queue-shaper queue <queue> <rate> [ kbps | mbps ] [ excess | credit ] [ rate-type { line | data } ]
```

```
qos shaper <rate> [ kbps | mbps ] [ rate-type { line | data } ]
```

	Argument	**Description**
Parameter	`<w0> <w1>…<w7>`	Weight for the specific queue 0–7 from 1 to 100.
	`<queue>`	Specific queue or range 0–7.
	`<rate>`	Controls the rate for the queue policer. This value is restricted to 100–3276700 when the unit is kbps, and 1–3276 when the unit is Mbps. The rate is internally rounded up to the nearest value supported by the queue police.
Default	NA	
Mode	Port List Interface mode	
Usage	Enable/Configure the Scheduler and Shapers for a specific port. Use the `no` version of the command to disable it.	

Example	Enable scheduler mode queue 0, 1, and 2 as 50 port 1 and set shaper rate as 100 Mbps operating on data rate.
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# qos wrr 50 50 50`
	`(config-if)# qos shaper 100 mbps rate-type data`	

3.17.5 QoS Egress Port Tag Remarking Configuration

Description
Use this command to configure tag remarking for all switch ports.

```
qos tag-remark { pcp <pcp> dei <dei> | mapped }
```

	Argument	**Description**
Parameter	`<pcp>`	Specific PCP 0–7
	`<dei>`	Specific DEI 0–1

.....continued		
	Argument	**Description**
	mapped	Use mapped versions of CoS and DPL.
Default	NA	
Mode	Port List Interface mode	
Usage	Configure tag remarking for a specific port. Use the no version of the command to go back to classified CoS and DPL values.	
Example	Configure tag remarking to default mode with PCP 5 and DEI 1. (config)# interface GigabitEthernet 1/1 (config-if)# qos tag-remark pcp 5 dei 1	

3.17.6 QoS Port DSCP Configuration

Description
Use this command to configure the basic QoS Port DSCP Configuration settings for all switch ports and enable/disable the Ingress Translation.

```
qos dscp-translate
```

```
qos dscp-classify { zero | selected | any }
```

```
qos dscp-remark { rewrite | remap | remap-dp }
```

	Argument	**Description**
Parameter	NA	NA
Default	Ingress Translation, classify, and remark disabled.	
Mode	Port List Interface mode	
Usage	Configure the basic QoS Port DSCP Configuration settings. Use the no version of the command to go back to default.	
Example	Enable translation and classify all DSCP on port 1. (config)# interface GigabitEthernet 1/1 (config-if)# qos dscp-translate (config-if)# qos dscp-classify any	

3.17.7 QoS DSCP-Based QoS Configuration

Description
Use this command to configure the basic QoS Port DSCP Configuration settings for all switch ports.

```
qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32
| af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos>
dpl <dpl>
```

	Argument	**Description**
Parameter	<dscp_num>	Specific DSCP or range. Maximum number of supported DSCP values are 64.
	<cos>	CoS value can be in the range of 0–7.
	<dpl>	Drop Precedence Level (range of 0–1).
Default	NA	

.....continued		
	Argument	**Description**
Mode	Global Configuration mode	
Usage	Configure basic QoS Port DSCP Configuration settings and trust. Use the `no` version of the command to disable trust.	

Example	1. Configure DSCP 8 (CS1) as trusted with CoS 3 and DPL 1.
	`(config)# qos map dscp-cos 8 cos 3 dpl 1`
	2. Remove trust of DSCP 8.
	`(config)# no qos map dscp-cos 8`	

3.17.8 QoS DSCP Translation Configuration

Description
Use this command to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

```
qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 |
af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef
| va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
```

```
qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
```

```
qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23
| af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef
| va } } <dpl> to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
```

	Argument	**Description**
Parameter	`<dscp_num>`	Specific DSCP or range. Maximum number of supported DSCP values are 64.
	`<dscp_num_tr>`	DSCP can be translated to any of (0–63) DSCP values.
	`<dpl>`	Drop Precedence Level (0–1).
Default	NA	
Mode	Global Configuration mode	
Usage	Configure QoS DSCP Translation. Use the `no` version of the command to remove the translation.	

Example	Configure DSCP 8 (CS1) translation to 10 (AF11) and enable classification at Ingress side.
	`(config)# qos map dscp-ingress translation cs1 to af11`
	`(config)# qos map dscp-classify 8`	

3.17.9 QoS DSCP Classification Configuration

Description
Use this command to configure the mapping of CoS and DPL to DSCP value.

```
qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22
| af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 |
ef | va } }
```

	Argument	Description
Parameter	<cos>	Actual Class of Service 0–7.
	<dpl>	Drop Precedence Level 0 or 1.
	<dscp_num>	Classified DSCP value 0–63.
Default	All CoS classified as 0 (BE).	
Mode	Global Configuration mode.	
Usage	Configure QoS DSCP Classification. Use the no version of the command to revert to default.	

Example	1. Configure CoS 5 DSCP DP0 to CS1 and DP1 to AF11.
	`(config)# qos map cos-dscp 5 dpl 0 dscp cs1`
	`(config)# qos map cos-dscp 5 dpl 1 dscp af11`
	2. Revert CoS 5 dpl1 to default
	`(config)# no qos map cos-dscp 5 dpl 1`	

3.17.10 QoS Control List Configuration

Description
Use this command to configure QoS Control List (QCL), which is made up of the QCEs. Define the QCE parameters. By default, all ports are included. **Default** means that the default classified value is not modified by this QCE.

```
qos qce { [ update ] } <qce_id> [ { next <qce_id_next> } | last ] [ interface <port_type>
[ <port_list> ] ] [ smac { <smac> | <smac_24> | any } ] [ dmac { <dmac> | unicast | multicast
| broadcast | any } ] [ tag { [ type { untagged | tagged | c-tagged | s-tagged | any } ]
[ vid { <ot_vid> | any } ] [ pcp { <ot_pcp> | any } ] [ dei { <ot_dei> | any } ] } ] [ inner-
tag { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <it_vid> | any } ]
[ pcp { <it_pcp> | any } ] [ dei { <it_dei> | any } ] } ] [ frame-type { any | { etype
[ { <etype_type> | any } ] } | { llc [ dsap { <llc_dsap> | any } ] [ ssap { <llc_ssap> |
any } ] [ control { <llc_control> | any } ] } | { snap [ { <snap_data> | any } ] } | { ipv4
[ proto { <pr4> | tcp | udp | any } ] [ sip { <sip4> | any } ] [ dip { <dip4> | any } ]
[ dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 |
af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [ fragment
{ yes | no | any } ] [ sport { <sp4> | any } ] [ dport { <dp4> | any } ] } | { ipv6 [ proto
{ <pr6> | tcp | udp | any } ] [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] } } ]
[ action { [ cos { <action_cos> | default } ] [ dpl { <action_dpl> | default } ] [ pcp-dei
{ <action_pcp> <action_dei> | default } ] [ policy { <action_policy> | default } ]
```

	Argument	Description
Parameter	<qce_id>	QCE ID. The allowed range is 1 to 256
	<qce_id_next>	The next QCE ID. Insert the current QCE before the next QCE ID.
	<port_type>	Port type in Giga or 2.5 Giga Ethernet
	<port_list>	List of Port ID. For example, 1/1,3–5; 2/2–4, 6.
	<smac>	Source MAC address: xx-xx-xx-xx-xx-xx or **Any**.
	<dmac>	Destination MAC address: Possible values are **Unicast**, **Multicast**, **Broadcast**, **Specific** (xx-xx-xx-xx-xx-xx) or **Any**.
	<ot_vid>	Valid value of VLAN ID can be any value in the range 1-4095 or **Any**; user can enter either a specific value or a range of VIDs.
	<ot_pcp>	Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2–3, 4–5, 6–7, 0–3, 4–7) or **Any**
	<ot_dei>	Valid value of DEI can be 0, 1 or **Any**.
	<<it_vid>>	Valid value of Inner VLAN ID can be any value in the range 1-4095 or **Any**; user can enter either a specific value or a range of VIDs.
	<it_pcp>	Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0–1, 2–3, 4–5, 6–7, 0–3, 4–7) or **Any**.
	<it_dei>	Valid value of Inner DEI can be 0, 1, or **Any**.

.....continued		
	Argument	**Description**
	<etype_type>	Frame Type can have any of the following values: Any, EtherType, LLC, SNAP, IPv4, IPv6.
	<llc_dsap>	Valid Destination Service Access Point (DSAP) can vary from 0x00 to 0xFF or **Any**.
	<llc_ssap>	Valid Source Service Access Point (SSAP) can vary from 0x00 to 0xFF or **Any**.
	<llc_control>	Valid Control field can vary from 0x00 to 0xFF or **Any**.
	<snap_data>	Valid PID(that is, Ether Type) can be 0x0000-0xFFFF or **Any**.
	<pr4>	IP protocol number: (0–255, **TCP** or **UDP**) or **Any**.
	<sip4>	Specific Source IP address in value/mask format or **Any**. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255.
	<dip4>	Specific Destination IP address in value/mask format or **Any**.
	<dscp4>	Diffserv Code Point value (DSCP): It can be a specific value, range of values or **Any**. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
	<sp4>	Source TCP/UDP port:(0–65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP.
	<dp4>	Destination TCP/UDP port:(0–65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP.
	<pr6>	IP protocol number: (0–255, **TCP** or **UDP**) or **Any**.
	<sip6>	32 LS bits of IPv6 source address in value/mask format or **Any**.
	<dip6>	Specific Destination IP address in value/mask format or **Any**.
	<dscp6>	Diffserv Code Point value (DSCP): It can be a specific value, range of values or **Any**. DSCP values are in the range 0–63 including BE, CS1-CS7, EF, or AF11-AF43.
	<sp6>	Source TCP/UDP port:(0–65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP
	<dp6>	Destination TCP/UDP port: (0–65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP.
	<action_cos>	Class of Service: (0–7) or **Default**.
	<action_dpl>	Drop Precedence Level: (0–1) or **Default**.
	<action_pcp>	Priority Code Point: (0–7) or **Default**.
	<action_dei>	Drop Eligible Indicator: (0–1) or **Default**.
	<action_policy>	ACL Policy number: (0–63) or **Default**.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure QCE Key and Action parameters. Use the no version of the command to delete the specific QCE entry.	
Example	Create QCE entry ID1 on port 1. `(config)# qos qce 1 interface GigabitEthernet 1/1`	

3.17.11 QoS Storm Policing Configuration

Description
Use this command to configure Global storm policers for the switch. There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, that is, frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

```
qos storm { unicast | broadcast | multicast} <rate> [ fps | kfps | kbps | mbps ]
```

	Argument	Description
Parameter	`<rate>`	Controls the rate for the global storm policer. This value is restricted to 1–1024000 when the unit is fps and 1–1024 when the unit is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are 1, 2, 4, 8, 16, 32, 64, 128, 256, and 512 fps for rates ≤ 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, and 1024 kfps for rates > 512 fps.
Default	NA	
Mode	Configuration mode	
Usage	Enable and configure Global storm policers. Use the `no` version of the command to disable.	
Example	Enable unicast storm policer with 100 fps rate `(config)# qos storm unicast 100`	

3.17.12 QoS Weighted Random Early Detection Configuration

Description
Use this command to configure the Random Early Detection (RED) settings. Through different RED configuration for the queues, it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports in the switch.

```
qos wred queue <queue> min-fl <min_fl> max <max> [ fill-level ]
```

	Argument	Description
Parameter	`<queue>`	The queue number (CoS) for which the configuration below applies. Specific queue or range 0–7.
	`<min_fl>`	Controls the lower RED fill level threshold. If the queue filling level is below this threshold, then the drop probability is zero. This value is restricted to 0%–100%.
	`<max>`	Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1%–100%.
Default	NA	
Mode	Global Configuration mode	
Usage	Enable and configure Random Early Detection (RED) settings for a specific QoS queues. Use the `no` version of the command to disable it.	
Example	Enable RED for queues 1, 2, and 3 with lower fill level 20% and upper 40% `(config)# qos wred queue 1-3 min-fl 20 max 40`	

3.18 Mirroring Configuration

Description
Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

```
monitor session <session_number> [ destination { interface <port_type> [ <di_list> ] | remote
vlan <drvid>
```

```
reflector-port <port_type> <rportid> } | source { interface <port_type> [ <si_list> ] [ both
| rx | tx ] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [ both | rx | tx ] } ]
```

	Argument	Description
Parameter	<session_number>	MIRROR session number 1–5.
	<port_type>	Port type in Giga or 2.5 Giga
	<di_list>	List of destination Port ID. For example, 1/1–4.
	<drvid>	Remote MIRROR destination RMIRROR VLAN number.
	<rportid>	Reflector Port ID in the format of switch-no/port-no.
	<si_list>	List of source Port ID. For example, 1/1–4.
	<srvid>	Remote MIRROR source RMIRROR VLAN number.
	<source_vlan_list>	MIRROR source VLAN
Default	NA	
Mode	Global Configuration mode	
Usage	Enable and configure Mirroring. Use the no version of the command to disable it.	
Example	1. Enable Mirroring Session 1 and configure remote source VLAN 100 (config)# monitor session 1 (config)# monitor session 1 source remote vlan 100 2. Disable Mirroring Session 1 (config)# no monitor session 1	

3.19 UPnP Configuration

Description
Use this command to configure Universal Plug and Play (UPnP) to allow seamless device connections and simplify the implementation of networks in home (data sharing, communications, and entertainment) and corporate environments for simplified installation of computer components.

```
upnp
```

```
upnp advertising-duration <v_100_to_86400>
```

```
upnp ip-addressing-mode { dynamic | static }
```

```
upnp static interface vlan <v_vlan_id>
```

	Argument	Description
Parameter	<v_100_to_86400>	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they must receive an SSDP advertisement message from this switch. Valid values are in the range 100 to 86400 seconds. Default 100 seconds.
	dynamic | static	IP addressing mode. Dynamic: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address. Static: User specifies the IP interface VLAN for choosing the IP address of the switch device.
	<v_vlan_id>	The index of the specific IP VLAN interface. Valid configurable values range from 1 to 4095. Default value is 1.
Default	UPnP Enabled	
Mode	Global Configuration mode	
Usage	Enable and configure UPnP. Use the no version of the command to disable it.	
Example	Enable UPnP and set the advertising duration to 200 seconds. (config)# upnp (config)# upnp advertising-duration 200	

3.20 sFlow Configuration

Description
Use this command to configure sFlow receiver (sFlow collector) and per-port flow and counter samplers. sFlow configuration is not persisted to non-volatile memory, which means that a reboot disables sFlow sampling.

3.20.1 sFlow Agent/Receiver Configuration

Description
Use this command to specify the IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that identifies this agent over extended periods of time. It also configures the sFlow receiver, port, timeout, and datagram size.

```
sflow agent-ip { ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> }
```

```
sflow collector-address [ <ipv4_var> | <ipv6_var> | <domain_name> ]
```

```
sflow collector-port <collector_port>
```

```
sflow timeout <timeout>
```

```
sflow max-datagram-size <datagram_size>
```

	Argument	Description
Parameter	<v_ipv4_addr> <v_ipv6_addr>	The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that identifies this agent over extended periods of time. IPv4 and IPv6 addresses are supported. Defaults to IPv4 loopback address 127.0.0.1

.....continued		
	Argument	**Description**
	<ipv4_var> <ipv6_var> <domain_name>	The IP address or hostname of the sFlow receiver. IPv4 and IPv6 addresses are supported.
	<collector_port>	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
	<timeout>	The number of seconds remaining before sampling stops and the current sFlow owner is released. Valid range is 0 to 2147483647 seconds with default 0 seconds.
	<datagram_size>	The maximum number of data bytes that can be sent in a single sample datagram. Valid range is 200 to 1468 bytes with default 1400 bytes.
Default	NA	
Mode	Global Configuration mode	
Usage	Configure sFlow Agent/Receiver parameters. Use the no version of the command to revert to default values.	
Example	Set sFlow receiver address 192.168.0.40, UDP port to 6232. (config)# sflow agent-ip 192.168.0.40 (config)# sflow collector-port 6232	

3.20.2 sFlow Port Configuration

Description
Use this command to enable or disable flow sampling and counter polling on the specific port, specify sampling rate, maximum header size and poling interval.

```
sflow
```

```
sflow sampling-rate <sampling_rate>
```

```
sflow max-sampling-size <max_sampling_size>
```

```
sflow counter-poll-interval <poll_interval>
```

	Argument	**Description**
Parameter	<sampling_rate>	The sample rate is specified as N to sample 1/Nth of the packets n the monitored flows. Valid range is 1 to 4096.
	<max_sampling_size>	The maximum number of bytes to transmit per flow sample. Valid range is 14 to 200 bytes with default 128 bytes.
	<poll_interval>	Specifies the interval in seconds between counter poller samples. Valid range is 1 to 3600 seconds.
Default	NA	
Mode	Port List Interface mode	
Usage	Enable flow sampling and specify parameters. Use the no version of the command to disable flow sampling or revert parameters to defaults.	

.....continued		
	Argument	**Description**

Example	Enable sFlow sampling on port 1 with sampling rate 400.
	`(config)# interface GigabitEthernet 1/1`
	`(config-if)# sflow`
	`(config-if)# sflow sampling-rate 400`	

4. Monitor Commands

This section describes all unit monitor pages.

4.1 System Monitor Commands

The following sections describe the Monitor system.

4.1.1 Monitor System Information

Description
Use this command to display the switch system information details.

```
show version
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display system information details.	
Example	# show version	

4.1.2 Monitor CPU load

Description
Use this command to display the switch CPU load status.

```
show system cpu status
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display system CPU status	
Example	# show system cpu status	

4.1.3 Monitor IP status

Description
Use this command to display the status of the IP protocol layer.

```
show interface vlan
```

```
show ip neighbor
```

```
show ipv6 neighbor
```

	Argument	Description
Parameter	NA	NA

.....continued		
	Argument	**Description**
Default	NA	
Mode	User EXEC mode	
Usage	Display the status of the IP protocol.	
Example	`# show interface vlan`	

4.1.4 Monitor IPv4 routing information base

Description
Use this command to display the IPv4 routing status.

```
show ip route
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display IPv4 routing information base.	
Example	`# show ip route`	

4.1.5 Monitor IPv6 Routing Information Base

Description
Use this command to display the IPv6 routing status.

```
show ipv6 route
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display IPv6 routing information base.	
Example	`# show ipv6 route`	

4.1.6 Monitor System Log

Description
Use this command to display the switch system log information up to 999 entries or filter by level.

```
show logging [ informational ] [ notice ] [ warning ] [ error ]
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display system log	

.....continued		
	Argument	**Description**
Example	Display only error log entries `# show logging error`	

4.1.7 Monitor Detailed System Log

Description
Use this command to display the switch system log information for a specific log entry.

```
show logging <log_id>
```

	Argument	**Description**
Parameter	`<log_id>`	The identification of the system log entry.
Default	NA	
Mode	User EXEC mode	
Usage	Display system specific log entry	
Example	Display log entry 20 `# show logging 20`	

4.2 Monitor Green Ethernet Port Power Savings

Description
Use this command to display the status for Energy Efficient Ethernet.

```
show green-ethernet
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display the status for port power savings.	
Example	`# show green-ethernet`	

4.3 Monitor Ports

Use these commands to display ports status information.

4.3.1 Monitor Ports State

Use this command to display the port state overview.

4.3.2 Monitor Port Statistics

Description
Use this command to display the general traffic statistics for all switch ports.

```
show interface <port_type> [ <port_list> ] statistics [ { packets | bytes | errors | discards
| filtered | { priority [ <priority_list> ] } | link-state-changes } ] [ { up | down } ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all)
	<port_list>	List of Port ID. For example, 1/1, 1/1–4.
	<priority_list>	Priority of the queue (or queues) to show statistics for.
Default	NA	
Mode	User EXEC Mode	
Usage	Display traffic statistics	
Example	Display traffic statistics for port 1 showing only errors. # show interface GigabitEthernet 1/1 statistics errors	

4.3.3 Monitor Port QoS, QCL Status, and Detailed Statistics

Description
Use this command to display statistics for the different queues for all switch ports.

```
show qos [ { interface [ <port_type> [ <port> ] ] } | wred | { maps [ dscp-cos ] [ dscp-
ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] | storm |
{ qce [ <qce> ] } ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all)
	<port>	List of Port ID, ex, 1/1, 1/1–4.
	<qce>	Indicates the QCE ID 1–256.
Default	NA	
Mode	User EXEC mode	
Usage	Display QoS statistics.	
Example	Display QoS statistics for port 1 # show qos GigabitEthernet 1/1	

4.4 Monitor CFM Status

Description
Use this command to display CFM MEP and services status.

```
show cfm meps [ domain <md_name> ] [ service <ma_name> ] [ mep-id <mepid> ] [ details ]
```

```
show cfm services [ domain <md_name> ] [ service <ma_name> ] [ details ]
```

	Argument	Description
Parameter	<md_name>	Domain name to show information.

.....continued		
	Argument	**Description**
	<ma_name>	Service name to show information.
	<mepid>	Particular MEP-ID to show information.
Default	NA	
Mode	User EXEC mode	
Usage	Display CFM status	
Example	Display detailed CFM status # show cfm meps details	

4.5 Monitor APS Status

Description
Use this command to display the APS status.

```
show aps [ <inst_list> ] { [ statistics ] | [ details ] }
```

	Argument	**Description**
Parameter	<inst_list>	The range of APS instances.
Default	NA	
Mode	User EXEC mode	
Usage	Display APS status.	
Example	Display detailed APS status # show aps details	

4.6 Monitor ERPS Status

Description
Use this command to display the ERPS status.

```
show erps [ <inst_list> ] [ statistics ] [ details ]
```

	Argument	**Description**
Parameter	<inst_list>	List of ERPS instances
Default	NA	
Mode	User EXEC mode	
Usage	Display ERPS status	
Example	Display detailed ERPS status. # show erps details	

4.7 Monitor DHCPv4 Status

Use these commands to display status of the DHCPv4 instances.

4.7.1 Monitor DHCPv4 Snooping Table

Description
Use this command to display the Dynamic DHCP Snooping table.

```
show ip dhcp snooping table
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display the IP assigned information that is obtained from DHCP server except for local VLAN interface IP addresses.	
Example	`# show ip dhcp snooping table`	

4.7.2 Monitor DHCPv4 Detailed Statistics

Description
Use this command to display the DHCPv4 detailed statistics for all switchports.

```
show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward |
combined } [ interface <port_type> [ <in_port_list> ] ]
```

	Argument	Description
Parameter	`<port_type>`	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	`<in_port_list>`	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display dhcpv4 statistics.	
Example	Display dhcpv4 combined statistics for port 1. `# show ip dhcp detailed statistics combined interface GigabitEthernet 1/1`	

4.8 Monitor DHCPv6 Status

Use this command to display status of the DHCPv4 instances.

4.8.1 Monitor DHCPv6 Snooping Table

Description
Use this command to display Dynamic DHCPv6 Snooping table.

```
show ipv6 dhcp snooping table [ all ]
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display the currently known DHCPv6 clients and their assigned addresses.	

.....continued		
	Argument	**Description**
Example	Show table of known DHCP clients with assigned addresses and show clients currently acquiring an address. `# show ipv6 dhcp snooping table all`	

4.8.2 Monitor DHCPv6 Snooping Statistics

Description
Use this command to display DHCPv6 snooping statistics for all switchports.

```
show ipv6 dhcp snooping statistics [ interface <port_type> [ <in_port_list> ] ] [ zero-
suppress ]
```

	Argument	**Description**
Parameter	`<port_type>`	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	`<in_port_list>`	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display dhcpv6 statistics.	
Example	Display dhcpv6 snooping statistics for port 1. `# show ip dhcp detailed statistics interface GigabitEthernet 1/1`	

4.9 Monitor Security Status

Use these commands to display the status of the security.

4.9.1 Monitor Access Management Statistics

Description
Use this command to display statistics for access management.

```
show access management statistics
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display the access management statistic.	
Example	`# show access management statistics`	

4.9.2 Monitor Security Network

The following sections describe the Monitor Security Network.

4.9.2.1 Monitor Security Network Port Security

The following sections describe the Monitor Security Network Port Security.

4.9.2.1.1 Monitor Security Network Port Security Overview

Description
Use this command to display the Port Security Switch Status overview.

```
show port-security [ interface <port_type> [ <plist> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<plist>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display Port Security overview status.	
Example	Display port security overview status for port 1. # show port-security interface GigabitEthernet 1/1	

4.9.2.1.2 Monitor Network Port Security Details

Description
Use this command to display the MAC Addresses learned by Port Security.

```
show port-security address [ interface <port_type> [ <plist> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<plist>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display MAC Addresses learned by Port Security.	
Example	Display port security overview status for port 1 # show port-security interface GigabitEthernet 1/1	

4.9.2.2 Monitor Security Network NAS

The following sections describe the Monitor Security Network NAS.

4.9.2.2.1 Monitor Security Network Access Server Switch Status

Description
Use this command to display Network Access Server Switch Status.

```
show dot1x status [ brief ]
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display NAS switch status	
Example	Display NAS status in a brief format # show dot1x status brief	

4.9.2.2.2 Monitor Security Network NAS Port

Description
Use this command to display detailed NAS statistics for a specific switch port.

```
show dot1x status [ interface <port_type> [ <v_port_type_list> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<v_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display NAS switch status	
Example	Display NAS status for port 1. # show dot1x status interface GigabitEthernet 1/1	

4.9.2.3 Monitor Security Network ACL-Status

Description
Use this command to display the ACL status by different ACL users.

```
show access-list ace-status [ static ] [ loop-protect ] [ dhcp ] [ dhcp6-snooping ] [ upnp ]
[ arp-inspection ] [ cfm ] [ aps ] [ erps ] [ ip-source-guard ] [ ipv6-source-guard ] [ ip ]
[ conflicts ]
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display ACL status by different ACL users.	
Example	Display ACL combined status # show access-list ace-status	

4.9.2.4 Monitor Security Network ARP Inspection

Description
Use this command to display entries in the Dynamic ARP Inspection table.

```
show ip arp inspection [ interface <port_type> [ <in_port_type_list> ] | vlan <in_vlan_list> ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<in_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
	<in_vlan_list>	Select a VLAN ID.
Default	NA	
Mode	User EXEC mode	
Usage	Display ARP Inspection table.	
Example	Display ARP inspection table. # show ip arp inspection	

4.9.2.5 Monitor Security Network IP Source Guard

Description
Use this command to display entries in the Dynamic IP Source Guard table.

```
show ip source binding [ dhcp-snooping | static ] [ interface <port_type>
[ <in_port_type_list> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<in_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display Dynamic IP Source Guard table.	
Example	Display Dynamic IP Source Guard table # show ip source binding	

4.9.2.6 Monitor Security Network IPv6 Source Guard

Description
Use this command to display entries in the Dynamic IPv6 Source Guard table.

```
show ipv6 source binding [ dhcpv6-snooping | static ] [ interface <port_type>
[ <port_list> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<in_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display Dynamic IPv6 Source Guard table.	
Example	Display Dynamic IPv6 Source Guard table # show ipv6 source binding	

4.9.3 Monitor Security AAA

The following sections describe the Monitor Security AAA.

4.9.3.1 Monitor Security AAA RADIUS Overview

Description
Use this command to display an overview of the status of the RADIUS servers.

```
show radius-server
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display RADIUS server status.	

.....continued		
	Argument	**Description**
Example	Display RADIUS server status. `# show radius-server`	

4.9.3.2 Monitor Security AAA RADIUS Details

Description
Use this command to display detailed status of the RADIUS servers.

```
show radius-server statistics
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display RADIUS server detailed status	
Example	Display RADIUS server detailed status. `# show radius-server statistics`	

4.9.4 Monitor Security Switch

The following sections describe the Monitor Security Switch.

4.9.4.1 Monitor Security Switch RMON

This section describes the Monitor Security switch RMON.

4.9.4.1.1 Monitor Security Switch RMON Statistics

Description
Use this command to display an overview of RMON Statistics entries.

```
show rmon statistics [ <id_list> ]
```

	Argument	**Description**
Parameter	`<id_list>`	Statistics entry list
Default	NA	
Mode	User EXEC mode	
Usage	Display RMON Statistics.	
Example	Display RMON Statistics for ID1. `# show rmon statistics 1`	

4.9.4.1.2 Monitor Security Switch RMON History

Description
Use this command to display an overview of RMON History entries.

```
show rmon history [ <id_list> ]
```

	Argument	**Description**
Parameter	`<id_list>`	History entry list

.....continued		
	Argument	**Description**
Default	NA	
Mode	User EXEC mode	
Usage	Display RMON History	
Example	Display RMON History for ID1. `# show rmon history 1`	

4.9.4.1.3 Monitor Security Switch RMON Alarm

Description
Use this command to display an overview of RMON Alarm entries.

```
show rmon alarm [ <id_list> ]
```

	Argument	**Description**
Parameter	`<id_list>`	Alarm entry list
Default	NA	
Mode	User EXEC mode	
Usage	Display RMON Alarm	
Example	Display RMON Alarm for ID1. `# show rmon alarm 1`	

4.9.4.1.4 Monitor Security Switch RMON Event

Description
Use this command to display an overview of RMON Event entries.

```
show rmon event [ <id_list> ]
```

	Argument	**Description**
Parameter	`<id_list>`	Event entry list
Default	NA	
Mode	User EXEC mode	
Usage	Display RMON Event	
Example	Display RMON Event for ID1. `# show rmon event 1`	

4.10 Monitor Aggregation

The following sections describe the Monitor Aggregation.

4.10.1 Monitor Aggregation Status

Description
Use this command to display the status of ports in Aggregation group.

```
show aggregation
```

	Parameter	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display Aggregation status	
Example	Display Aggregation status. `# show aggregation`	

4.10.2 Monitor Aggregation LACP

The following sections describe the Monitor Aggregation LACP.

4.10.2.1 Monitor Aggregation LACP System Status

Description

Use this command to display the status overview for the system-level LACP information.

```
show lacp system-id [ details ]
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display system-level LACP information.	
Example	Display system-level LACP detailed info `# show lacp system-id details`	

4.10.2.2 Monitor Aggregation LACP Internal Status

Description

Use this command to display an overview for the LACP internal status for all ports.

```
show lacp internal [ details ]
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display internal LACP information	
Example	Display internal LACP detailed info `# show lacp internal details`	

4.10.2.3 Monitor Aggregation LACP Neighbor Status

Description

Use this command to display an overview for the LACP neighbor status for all ports.

```
show lacp neighbor [ details ]
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display LACP neighbor information	
Example	Display LACP neighbor detailed info # show lacp neighbor details	

4.10.2.4 Monitor Aggregation LACP Port Statistics

Description
Use this command to display an overview for the LACP statistics for all ports.

```
show lacp statistics [ details ]
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display LACP statistics information	
Example	Display LACP detailed statistics # show lacp statistics details	

4.11 Monitor Loop Protection

Description
Use this command to display the loop protection port status the ports of the switch.

```
show loop-protect [ interface <port_type> [ <plist> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<plist>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display loop protection status	
Example	Display loop protection status for port 1 # show loop-protect interface GigabitEthernet 1/1	

4.12 Monitor Spanning Tree

The following sections describe the Monitor Spanning Tree.

4.12.1 Monitor Spanning Tree Bridge Status

Description
Use this command to display the status overview of all STP bridge instances.

```
show spanning-tree active
```

	Argument	Description
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display status of STP bridge instances	
Example	Display status of STP bridge instances. `# show spanning-tree active`	

4.12.2 Monitor Spanning Tree Port Status

Description
Use this command to display the STP CIST port status for physical ports of the switch.

```
show spanning-tree interface <port_type> [ <v_port_type_list> ]
```

	Argument	Description
Parameter	`<port_type>`	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	`<v_port_type_list>`	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display STP status	
Example	Display STP status for port 1 `# show spanning-tree interface GigabitEthernet 1/1`	

4.12.3 Monitor Spanning Tree Port Statistics

Description
Use this command to display the STP port statistics counters of bridge ports in the switch.

```
show spanning-tree detailed interface <port_type> [ <v_port_type_list> ]
```

	Argument	Description
Parameter	`<port_type>`	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	`<v_port_type_list>`	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display detailed STP status	
Example	Display detailed STP status for port 1 `# show spanning-tree detailed interface GigabitEthernet 1/1`	

4.13 Monitor LLDP

The following sections describe the Monitor LLDPs.

4.13.1 Monitor LLDP Neighbors

Description
Use this command to display the status overview for all LLDP neighbors.

```
show lldp neighbors [ interface <port_type> [ <v_port_type_list> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<v_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display LLDP neighbors status.	
Example	Display LLDP status for port 1. # show lldp neighbors interface GigabitEthernet 1/1	

4.13.2 Monitor LLDP LLDP-MED Neighbors

Description
Use this command to display the status overview of all LLDP-MED neighbors.

```
show lldp med remote-device [ interface <port_type> [ <port_list> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<v_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display LLDP-MED neighbors status.	
Example	Display LLDP-MED status for port 1 # show lldp med remote-device interface GigabitEthernet 1/1	

4.13.3 Monitor LLDP EEE

Description
Use this command to display the status of LLDP EEE.

```
show lldp eee [ interface <port_type> [ <v_port_type_list> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<v_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display LLDP EEE status	

.....continued		
	Argument	**Description**
Example	Display LLDP EEE status for port 1 # show lldp eee interface GigabitEthernet 1/1	

4.13.4 Monitor LLDP Port Statistics

Description
Use this command to display LLDP statistics for all switchports.

```
show lldp statistics [ interface <port_type> [ <v_port_type_list> ] ]
```

	Argument	**Description**
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all)
	<v_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display LLDP port statistics	
Example	Display LLDP statistics for port 1 # show lldp statistics interface GigabitEthernet 1/1	

4.14 Monitor PoE

Description
Use this command to display the PoE status of all switchports.

```
show poe [ interface <port_type> [ <v_port_type_list> ] ]
```

	Argument	**Description**
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<v_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display PoE status	
Example	Display LLDP statistics for port 1 # show poe interface GigabitEthernet 1/1	

4.15 Monitor MAC Table

Description
Use this command to display the entries in the MAC table.

```
show mac address-table
```

	Argument	**Description**
Parameter	NA	NA

.....continued		
	Argument	**Description**
Default	NA	
Mode	User EXEC mode	
Usage	Display status of STP bridge instances.	
Example	Display status of STP bridge instances. `# show spanning-tree active`	

4.16 Monitor VLANs

The following sections describe the Monitor VLANs.

4.16.1 Monitor VLANs Membership

Description

Use this command to display an overview of membership status of VLAN users.

```
show vlan status [ admin | all | combined | nas | rmirror ]
```

	Argument	**Description**
Parameter	NA	NA
Default	NA	
Mode	User EXEC mode	
Usage	Display the membership status of VLAN users.	
Example	Display VLAN membership status for combined users. `# show vlan status combined`	

4.16.2 Monitor VLAN Ports

Description

Use this command to display the VLAN port status.

```
show vlan status [ interface <port_type> [ <plist> ] ] [ admin | all | combined | erps | mstp
| nas | rmirror ]
```

	Argument	**Description**
Parameter	`<port_type>`	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all)
	`<plist>`	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display VLAN port status	
Example	Display VLAN port 1 status for admin user `# show vlan status interface GigabitEthernet 1/1 admin`	

4.17 Monitor sFlow

Description
Use this command to display receiver and per-port sFlow statistics.

```
show sflow statistics [ receiver | samplers [ interface <port_type> [ <v_port_type_list> ] ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<v_port_type_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Display sFlow statistics	
Example	Display sFlow statistics # show sflow statistics samplers interface GigabitEthernet 1/1	

5. Diagnostics

This section describes the Network assist tools, such as ping and trace route. Also measure Ethernet cable lengths.

5.1 Diagnostics Ping (IPv4)

Description

Use this command to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.

```
ping [ ip ] { <domain_name> | <ip_addr> } [ ttl <ttl_value> ] [ repeat <count> ] [ { saddr
<src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } } ] [ size <size> ] [ data
<data_value> ] [ { verbose | quiet } ]
```

	Argument	Description
Parameter	<domain_name>	Destination hostname or FQDN
	<ip_addr>	Destination IPv4 address
	<ttl_value>	IPv4 TTL: 1–255; Default is 64.
	<count>	Packets: 1–60; Default is 5.
	<src_addr>	Source Address of interface
	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet.
	<src_if>	Port ID in the format of switch-no/port-no.
	<vlan_id>	Source VLAN interface
	<size>	Size (bytes): 2–1452; Default is 56.
	<data_value>	Payload data: 0–255; Default is 0
Default	NA	
Mode	User EXEC mode	
Usage	Send ICMP echo messages	
Example	Send ten pings to 192.168.0.2 # ping ip 192.168.0.2 count 10	

5.2 Diagnostics Ping (IPv6)

Description

Use this command to issue ICMP (IPv6) PING packets to troubleshoot IP connectivity issues.

```
ping ipv6 { <domain_name> | <ip_addr> } [ repeat <count> ] [ saddr <src_addr> ] [ sif
{ <port_type> <src_if> | vlan <vlan_id> } ] [ size <size> ] [ data <data_value> ] [ { verbose
| quiet } ]
```

	Argument	Description
Parameter	<domain_name>	Destination hostname or FQDN.
	<ip_addr>	Destination IPv6 address.
	<count>	Packets: 1–60; Default is 5.
	<src_addr>	Source Address of interface.
	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet.
	<src_if>	Port ID in the format of switch-no/port-no.
	<vlan_id>	Source VLAN interface.

.....continued		
	Argument	**Description**
	<size>	Size (bytes): 2–1452; Default is 56.
	<data_value>	Payload data: 0–255; Default is 0.
Default	NA	
Mode	User EXEC mode	
Usage	Send ICMPv6 echo messages	
Example	Send ten pings to 2001:db8:: `# ping ip 2001:db8:: count 10`	

5.3 Diagnostics—Traceroute (IPv4)

Description
Use this command to perform a Traceroute test over IPv4 towards a remote host.

```
traceroute ip { <domain_name> | <ip_addr> } [ dscp <dscp> ] [ timeout <timeout> ] [ { saddr
<src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } } ] [ probes <probes> ] [ firstttl
<firstttl> ] [ maxttl <maxttl> ] [ icmp ] [ numeric ]
```

	Argument	**Description**
Parameter	<domain_name>	Destination hostname or FQDN
	<ip_addr>	Destination IPv4 address
	<dscp>	DSCP value (decimal value, default 0)
	<timeout>	Time to wait for a response in seconds (default 3)
	<src_addr>	Source Address of interface
	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet
	<src_if>	Port ID in the format of switch-no/port-no
	<vlan_id>	Source VLAN interface
	<probes>	Number of probes per hop (default 3)
	<firstttl>	First number of hops (default 1)
	<maxttl>	Max number of hops (default 30)
Default	NA	
Mode	User EXEC mode	
Usage	Perform a Traceroute test	
Example	Traceroute to 192.168.0.2 with 5 probes. `# traceroute ip 192.168.0.2 probes 5`	

5.4 Diagnostics—Traceroute (IPv6)

Description
Use this command to perform a Traceroute test over IPv6 towards a remote host.

```
traceroute ipv6 { <domain_name> | <ip_addr> } [ dscp <dscp> ] [ timeout <timeout> ] [ saddr
<src_addr> ] [ sif { <port_type> <src_if> | vlan <vlan_id> } ] [ probes <probes> ] [ maxttl
<maxttl> ] [ numeric ]
```

	Argument	Description
Parameter	<domain_name>	Destination hostname or FQDN
	<ip_addr>	Destination IPv6 address
	<dscp>	DSCP value (decimal value, default 0)
	<timeout>	Time to wait for a response in seconds (default 3)
	<src_addr>	Source Address of interface
	<port_type>	Port type in Gigabit Ethernet, 2.5Gigabit Ethernet
	<src_if>	Port ID in the format of switch-no/port-no
	<vlan_id>	Source VLAN interface
	<probes>	Number of probes per hop (default 3)
	<maxttl>	Max number of hops (default 30)
Default	NA	
Mode	User EXEC mode	
Usage	Perform a Traceroute test	
Example	Traceroute to 2001:db8:: with 5 probes. `# traceroute ipv6 2001:db8::probes 5`	

5.5 Diagnostics VeriPHY

Description
Use this command to perform the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

```
veriphy [ { interface <port_type> [ <port_list> ] } ]
```

	Argument	Description
Parameter	<port_type>	Port type in Gigabit Ethernet, 2.5 Gigabit Ethernet or * (for all).
	<port_list>	List of Port ID. For example, 1/1, 1/1–4.
Default	NA	
Mode	User EXEC mode	
Usage	Run VeriPHY cable diagnostics	
Example	Perform VeriPHY cable diagnostics on port 1. `# veriphy interface GigabitEthernet 1/1`	

6. Maintenance

This section describes maintenance activities, such as resetting the device, restore configuration to factory default, software update, and unit configuration.

6.1 Restart Device

Description

Use this command to perform unit's software reset. After restart, the switch boots normally.

```
reload cold
```

	Argument	Description
Parameter	—	—
Default	NA	
Mode	EXEC	
Usage	Use this command to restart the unit.	
Example	`# reload cold`	

6.2 Factory Defaults

Description

Use this command to restore full factory default configuration. Only IP configuration is retained.

```
reload defaults
```

	Argument	Description
Parameter	—	—
Default	NA	
Mode	EXEC	
Usage	Use this command to restore to factory default.	
Example	`# reload defaults`	

6.3 Maintenance Software

The following sections describe the maintenance software.

6.3.1 Software Upload

Description

Use this command to update the firmware that controls the switch.

```
firmware upgrade <url_file>
```

	Argument	Description
Parameter	<url_file>	Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the following special characters: space !\"#$%&'()*+,/:;<=>?@[\\]^`{|}~ must be contained in the input URL string. They must be percent-encoded. A valid file name is a text string drawn from alphabet (A–Z, a–z), digits (0–9), dot (.), hyphen (-), and under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains (.) is not allowed.
Default	NA	
Mode	EXEC	
Usage	Use this command to upload the firmware from TFTP Server to unit local file.	
Example	Upload firmware file test.mfi from TFTP server. # firmware upgrade tftp://192.168.0.40/test.mfi	

6.3.2 Image Select

Description
Use this command to swap the active and alternative (back-up) firmware images.

```
firmware swap
```

	Argument	Description
Parameter	—	—
Default	NA	
Mode	EXEC	
Usage	Use this command to swap the active and alternate firmware images.	
Example	# firmware swap	

6.4 Maintenance—Configuration

The following sections describe the maintenance configurations.

6.4.1 Configuration Save startup-config

Description
Use this command to save running-config to startup-config and ensures that the currently active configuration is used at the next reboot.

```
copy running-config startup-config
```

	Argument	Description
Parameter	—	—
Default	NA	
Mode	EXEC	

.....continued		
	Argument	**Description**
Usage	Use this command to save unit configuration	
Example	`# copy running-config startup-config`	

6.4.2 Configuration Download

Description
Use this command to save running (or startup) configuration files to another file name or to TFTP server.

```
copy <running config | startup-config | flash:file-name | tftp://server/filename>
```

	Argument	**Description**
Parameter	—	—
Default	NA	
Mode	EXEC	
Usage	Use this command to copy unit configuration to another file or to TFTP server or from TFTP server to unit local file.	

Example	1. Save current configuration stored in unit flash to another file named **test** also inside unit FLASH.
	`# copy running-config flash:test`
	2. Save unit running configuration file to TFTP Server under name **test**
	`# copy running-config tftp://192.168.0.40/test`	

6.4.3 Configuration Upload

Description
Use this command to upload a file from the TFTP server to all the files on the switch, except `default-config`, which is read-only.

```
copy <tftp://server/filename > { startup-config | running-config | < flash:filename> }
```

	Argument	**Description**
Parameter	—	—
Default	NA	
Mode	EXEC	
Usage	Use this command to upload a configuration file from the TFTP server to another file on the switch.	
Example	Upload unit configuration file **test** from TFTP Server to startup-config file. `# copy tftp://192.168.0.40/test startup-config`	

6.4.4 Configuration Activate

Description
Use this command to activate any configuration file present on the switch, except for `running-config`, which represents the currently active configuration.

```
copy <flash:filename> running-config
```

	Argument	Description
Parameter	`<flash:filename>`	File in FLASH
Default	NA	
Mode	EXEC	
Usage	Use this command to activate a configuration file on the switch.	
Example	Activate configuration file **test** `# copy test running-config`	

6.4.5 Delete Configuration File

Description
Use this command to delete any writable configuration file stored in flash, including `startup-config`.

```
delete <path>
```

	Argument	Description
Parameter	`<path>`	File in FLASH. Syntax: `<flash:filename>`. A valid file name is a text string drawn from alphabet (A–Z, a–z), digits (0–9), dot (.), hyphen (-), and under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains (.) is not allowed.
Default	NA	
Mode	EXEC	
Usage	Use this command to delete unit configuration stored in flash.	
Example	`# del flash:test`	

7. Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Revision	Date	Description
A	03/2023	Initial revision

Microchip Information

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded

by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, KoD, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

ISBN: 978-1-6683-2076-1

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820