Command Line Interface

USER GUIDE

SZ2G-0416IXS
SZ2G-0416IXSP
SZ2G-0424IXS
SZ2G-0424IXSP

1. AAA

1.1. aaa authentication

Item	Description
Syntax	aaa authentication (login | enable) (default | LISTNAME) METHODLIST [METHODLIST] [METHODLIST] [METHODLIST]
	no aaa authentication (login | enable) LISTNAME
	Login: Login: Add/Edit login authentication list
	Enable: Add/Edit enable authentication list
	Default: Default: Edit default authentication list
	LISTNAME: Specify the list name for authentication type
	METHODLIST: Specify the authenticate method, including none, local,enable, tacacs+, radius.
Default	Default authentication list name for type login is “default” and default method is “local”. Default authentication list name for type enable is “default” and default method is “enable
Mode	Global Configuration
Usage	Login authentication is used when user try to login into the switch. Such as CLI login dialog and WEBUI login web page. Enable authentication is used only on CLI for user trying to switch from User EXEC mode to Privileged EXEC mode. Both of them support following authenticate methods. Local: Use local user account database to authenticate. (This method is not supported for enable authentication) Enable: Use local enable password database to authenticate. Tacacs+: Use remote Tacas+ server to authenticate. Radius: Use remote Radius server to authenticate. None: Do nothing and just make user to be authenticated. Each list allows you to combine these methods with different orders. For example, we want to authenticate login user with remote Tacacs+ server, but server may be crashed. Therefore, we need a backup plan, such as another Radius server. So we can configure the list with Tacacs+ server as first authentication method and Radius server as second one. Use no form to delete the existing list. However, “default” list is not allowed to remove.

Example:

This example shows how to add a login authentication list to authenticate with order tacacs+, radius, local.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
```

This example shows how to show existing login authentication lists .

```
Switch# show aaa authentication login lists
    Login List Name | Authentication Method List
        ----------------+------------------------------
            default | local
            test1   | tacacs+   radius  local
```

This example shows how to add an enable authentication list to authenticate with order tacacs+, radius, enable.

```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
```

This example shows how to show existing enable authentication lists.

```
 Switch# show aaa authentication login lists
     Enable List Name | Authentication Method List
        -------------+------------------------------
            Default    | enable
            test2      | tacacs+    radius  enable
```

1.2. login authentication

Item	Description
Syntax	login authentication LISTNAME
	no login authentication
	LISTNAME: Specify the login authentication list name to use.
Default	Default login authentication list for each line is “default”.
Mode	Line Configuration
Usage	Different access methods are allowed to bind different login authentication lists. Use “login authentication” command to bind the list to specific line (console, telnet, ssh). Use no form to bind the “default” list back.

Example:

This example shows how to create a new login authentication list and bind to telnet line.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# line telnet
```

```
Switch(config-line)# login authentication test1

This example shows how to show line binding lists.
Switch# show line lists
Line Type   |   AAA Type    |   List Name
-----------+---------------+-----------------
   console |     login     | default
           |    enable     | default
   telnet  |     login     | test1
           |   enable      | default
     ssh   |     login     | default
           |     enable    | default
     http  |     login     | default
     https |   login       | default
```

1.3. ip http login authentication

Item	Description
Syntax	ip (http | https) login authentication LISTNAME
	no ip (http | https) login authentication
Parameter	**http**：Bind login authentication list to user access WEBUI with http protocol
	https: Bind login authentication list to user access WEBUI with https protocol
	LISTNAME: Specify the login authentication list name to use.
Default	Default login authentication list for each line is “default”.
Mode	Global Configuration
Usage	Different access methods are allowed to bind different login authentication lists. Use “ip (http | https) login authentication” command to bind the list to WEBUI access from http or https. Use no form to bind the “default” list back.

Example:

This example shows how to create two new login authentication lists and bind to http and https.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# aaa authentication login test2 radius local
Switch(config)# ip http login authentication test1
Switch(config)# ip https login authentication test2

This example shows how to show line binding lists.
Switch# show line lists
```

```
Line Type   |   AAA Type    |   List Name
------------+--------------+-----------------
    console |     login      | default
            |     enable     | default
    telnet  |     login      | default
            |     enable     | default
        ssh |     login      | default
            |     enable     | default
       http |     login      | test1
      https |     login      | test2
```

1.4. enable authentication

Item	Description
Syntax	enable authentication LISTNAME
	no enable authentication
Parameter	**LISTNAME:** Specify the enable authentication list name to use.
Default	Default enable authentication list for each line is “default”.
Mode	Line Configuration.
Usage	Different access methods are allowed to bind different enable authentication lists. Use “enable authentication” command to bind the list to specific line (console, telnet, ssh). Use no form to bind the “default” list back.

Example:

This example shows how to create a new enable authentication list and bind to telnet line.

```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
Switch(config)# line telnet
Switch(config-line)# enable authentication test1
```

```
This example shows how to show line binding lists.
Switch# show line lists
Line Type   |   AAA Type    |   List Name
------------+--------------+-----------------
   console  |     login     | default
            |   enable      | default
   telnet   |    login      | default
            |   enable      | test1
       ssh  |    login      | default
            |   enable      | default
```

```
http |   login      | default
https |  login      | default
```

1.5. show aaa authentication

Item	Description
Syntax	show aaa authentication (login | enable) lists
Parameter	**Login**: Show login authentication list
	Enable: Show enable authentication list
Default	No default value for this command
Mode	Privileged EXEC
Usage	Use "show aaa authentication" command to show login authentication or enable authentication method lists.

Example:

This example shows how to show existing login authentication lists.

```
Switch# show aaa authentication login lists
Login List Name| Authentication Method List
----------------+------------------------------
default | local
test1   | tacacs+  radius  local

This example shows how to show existing enable authentication lists
Switch# show aaa authentication login lists
 Enable List Name | Authentication Method List
-----------------+------------------------------
       default   | enable
       test2     | tacacs+ radius  enable
```

1.6. show line lists

Item	Description
Syntax	show line lists
Parameter	
Default	No default value for this command
Mode	Privileged EXEC
Usage	Use "show line lists" command to show all lines' binding list of all authentication, authorization, and accounting function.

Example:

This example shows how to show line binding lists.

```
Switch# show line lists
Line Type   |   AAA Type    |   List Name
-----------+---------------+-----------------
    console |   login   | default
            |   enable  | default
    telnet  |   login   | default
            |   enable  | default
        ssh |   login   | default
            |   enable  | default
       http |   login   | default
     Https  |    login   | default
```

1.7. radius default-config

Item	Description
Syntax	radius default-config [key RADIUSKEY] [retransmit <1-10>] [timeout <1- 30>]
Parameter	**key RADIUSKEY:** Specify default radius server key string
	retransmit <1-10>: Specify default radius server retransmit value
	timeout <1-30>: Specify default radius server timeout value
Default	Default radius key is “”. Default radius retransmit is 3 times. Default radius timeout is 3 seconds.
Mode	Global Configuration
Usage	Use “radius default-config” command to modify default values of radius server. These default values will be used when user try to create a new radius server and not assigned these values.

Example:

```
This example shows how modify default radius configuration.
Switch(config)# radius default-config timeout 20
Switch(config)# radius default-config key radiuskey
Switch(config)# radius default-config retransmit 5
This example shows how to show default radius configurations.
Switch# show radius default-config
Retries| Timeout|  Key
--------+--------+---------
5   |   20  | radiuskey
```

This example shows how to create a new radius server with above default config and show results.

```
Switch(config)# radius host 192.168.1.111
Switch# show radius
Prio |  IP Address| Auth-Port|Acct-Port| Retries| Timeout| Type|Key
-----+-----------+----------+---------+--------+--------+-----+-----
1    |192.168.1.111 |  1812  | 1813    |    5   |  20    | All | radiuskey
```

1.8. radius host

Item	Description
Syntax	radius host HOSTNAME [auth-port <0-65535>][acct-port <0-65535>] [key RADIUSKEY] [priority <0-65535>] [retransmit <1-10>] [timeout <1-30>] [type (login|802.1x|all)
	no radius [host HOSTNAME]
Parameter	**host HOSTNAME:** Specify radius server host name, both IP address and domain name are available.
	auth-port <0-65535>: Specify radius server udp port
	acct-port <0-65535> : Specify radius Accounting udp port
	key RADIUSKEY: Specify radius server key string
	priority <0-65535>: Specify radius server priority
	retransmit <1-10>: Specify radius server retransmit times
	timeout <1-30>: Specify radius server timeout value
	Type(login|802.1X|all**):**Usage type of this server; Use for login; Use for 802.1X authentication;Use for both login and 802.1X authentication.
Default	Default radius key is “”.Default radius timeout is 3 seconds.
Mode	Global Configuration
Usage	Use “**radius host**” command to add or edit an existing radius server. Use no form to delete one or all radius servers from database.

Example:

This example shows how to create a new radius server.

```
Switch(config)# radius host 192.168.1.111 auth-port 12345 acct-port 12346
key radiuskey priority 100 retransmit 5 timeout 10 type all
```

This example shows how to show existing radius server.

```
Switch# show radius
```

```
Prio |IP Address| Auth-Port|Acct-Port|Retries|Timeout| Type| Key
-----+------------+-------+---------+------+-------+-----+---------
 1   | 192.168.1.111 |12345 | 12346   | 5     | 20   | All  | radiuskey
```

1.9. show radius default-config

Item	Description
Syntax	show radius default-config
Parameter	
Default	No default value for this command
Mode	Privileged EXEC
Usage	Use “show radius default-config” command to show radius default configurations.

Example:

This example shows how to show default radius configurations.

```
Switch# show radius default-config
Retries| Timeout|  Key
-------+--------+---------
  5    | 20     | radiuskey
```

1.10. show radius

Item	Description
Syntax	show radius
Parameter	
Default	No default value for this command
Mode	Privileged EXEC
Usage	Use “show radius” command to show existing radius servers.

Example:

This example shows how to show existing radius server.

```
Switch# show radius
Prio |IP Address| Auth-Port|Acct-Port| Retries|Timeout|Usage-Type|Key
-----+----------+----------+--------+--------+-----------+--------+---
 100 | 192.168.1.111|12345 |  12346 |    5   |   10    | All | radiuskey
```

1.11. show tacacs

Item	Description
Syntax	show tacacs
	show tacacs default-config
Parameter	
Default	No default value for this command
Mode	Privileged EXEC
Usage	Use "**show tacacs** " and "**show tacacs default-config**"command to show tacacs default configurations.

Example：

This example shows how to show tacacs configurations.

```
Switch# show tacacs
 Prio | Timeout |     IP Address     | Port  |   Key
------+---------+--------------------+-------+----------
Switch# show tacacs default-config
 Timeout|   Key
--------+---------
     5  |
```

1.12. tacacs default-config

Item	Description
Syntax	tacacs default-config [key TACPLUSKEY] [timeout <1-30>]
Parameter	**[key TACPLUSKEY]**: Tacacs+ server key
	[timeout <1-30>]: Tacacs+ server timeout
Default	
Mode	Global configuration
Usage	Use " **tacacs default-config**"command to set tacacs default configurations.

Example：

This example shows how to set tacacs configurations.

```
Switch(config)# tacacs default-config key aaa timeout 3
```

1.13. tacacs host

Item	Description
Syntax	tacacs host HOSTNAME [port <0-65535>] [key TACPLUSKEY] [priority <0-65535>] [timeout <1-30>]
	no tacacs host HOSTNAME
Parameter	**HOSTNAME**:Host name
	<0-65535>: TCP/UDP port number (0 ~ 65535)
	[key TACPLUSKEY]:Tacacs+ server key
	[priority <0-65535>]:Server priority vlaue in Server Group
	[timeout <1-30>]:Tacacs+ server timeout
Default	
Mode	Global configuration
Usage	Use " **tacacs host**"command to set tacacs+ server information. Use the **no** form of this command to restore to default setting.

Example：

This example shows how to set tacacs configurations.

```
Switch(config)# tacacs host test port 1 key key1 priority 1 timeout 1
DNS resolution failed. Please check DNS server setting or host name
```

2. ACL

2.1. mac acl

Item	Description
Syntax	mac acl NAME
	no mac acl NAME
Parameter	**NAME:** Specify the name of MAC ACL
Default	No default is defined
Mode	Global Configuration
Usage	Use the mac acl command to create a MAC access list and to enter mac-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit "deny any" ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Example:

The example shows how to create a mac acl. You can verify settings by the following show acl command.

Switch(config)# **mac acl test**

Switch(config-mac-acl)# **show acl**

MAC access list test

2.2. Permit(MAC)

Item	Description
Syntax	[sequence <1-2147483647>] permit(A:B:C:D:E:F/A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7><0-7>][ethtype <0x0600-0xFFFF>]
	no sequence <1-2147483647>
Parameter	**<1-2147483647>:** (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
	(A:B:C:D:E:F/A:B:C:D:E:F|any): Specify the source MAC address and mask of packet or any MAC address.
	(A:B:C:D:E:F/A:B:C:D:E:F|any): Specify the destination MAC address and mask of packet or any MAC address
	[vlan <1-4094>]: (Optional) Specify the vlan ID of packet.
	[cos <0-7> <0-7>]: (Optional) Specify the Class of Service value and mask of packet.

	[ethtype <0x0600-0xFFFF>]: (Optional) Specify Ethernet protocol number of packet
Default	No default is defined.
Mode	MAC ACL Configuration
Usage	Use the permit command to add permit conditions for a mac ACE that bypass those packets hit the ACE. The "sequence" also represents hit priority when ACL bind to an interface. An ACE not specifies "sequence" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE.

Example:

The example shows how to add an ACE that permit packets with source MAC address 22:33:44:55:66:77 、 VLAN 3 and Ethernet type 1999. You can verify settings by the following **show acl** command.

```
Switch(config)# mac acl test
Switch(config-mac-acl)# sequence 999 permit
22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 0x2800
Switch(config-mac-acl)# show acl
MAC access list test
sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype
0x2800
```

2.3. deny (MAC)

Item	Description
Syntax	[sequence <1-2147483647>] deny (A:B:C:D:E:F/A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7> <0-7>][ethtype <0x0600-0xFFFF>] [shutdown]
	no sequence <1-2147483647>
Parameter	**<1-2147483647>:** (Optional) Specify sequence
	(A:B:C:D:E:F/A:B:C:D:E:F|any): index of ACE, the sequence index represent the priority of an ACE in ACL.
	(A:B:C:D:E:F/A:B:C:D:E:F|any): Specify the source MAC address and mask of packet or any MAC address. Specify the destination MAC address and mask of packet or any MAC address.
	[vlan <1-4094>]: (Optional) Specify the vlan ID of packet.
	[cos <0-7> <0-7>]:(Optional) Specify the Class of Service value and mask of packet.

	[ethtype <0x0600-0xFFFF>]:(Optional) Specify Ethernet protocol number of packet.
	[shutdown]: (Optional) Shutdown interface while ACE hit
Default	No default is defined.
Mode	MAC ACL Configuration
Usage	Use the deny command to add deny conditions for a mac ACE that drop those packets hit the ACE. The "sequence" also represents hit priority when ACL bind to an interface. An ACE not specifies "sequence" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE. Use "shutdown" to shutdown interface while ACE hit.

Example:

The example shows how to add an ACE that denies packets with destination MAC address aa:bb:cc:xx:xx:xx and VLAN 9. You can verify settings by the following **show acl** command.

```
Switch(config)# mac acl test
Switch(config-mac-acl)# sequence 30 permit any any
Switch(config-mac-acl)# deny any aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 vlan 9 shutdown
Switch(config-mac-acl)# show acl
MAC access list test
sequence 30 permit any any
sequence 1019 deny any AA:BB:CC:00:00:00/FF:FF:FF:00:00:00 vlan 9 shutdown
```

2.4. ip acl

Item	Description
Syntax	ip acl NAME
	no ip acl NAME
Parameter	**<1-2147483647>:** (Optional) Specify sequence
	NAME: Specify the name of IPv4 ACL
Default	No default is defined.
Mode	Global Configuration
Usage	Use the **ip acl** command to create an IPv4 access list and to enter ip-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit "deny any" ACE created at the end of

	the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Example:

The example shows how to create an IP ACL. You can verify settings by the following **show acl** command.

```
Switch(config)#ip acl iptest
Switch(config-ip-acl)#show acl
  IP access list iptest
```

2.5. permit (IP)

Item	Description
Syntax	[sequence <1-2147483647>] permit (<0-255>|ipinip|egp|igp|hmp|rdp|ipv6| ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) [(dscp|precedence) VALUE]]
	[sequence <1-2147483647>] permit icmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (<0-255>|echo-reply|destination-unreachable|source-quench|echo-request|router-advertisement|router-solicitation|time-exceeded|timestamp| timestamp-reply|traceroute|any) (<0- 255>|any) [(dscp|precedence) VALUE]
	[sequence <1-2147483647>] permit tcp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo| discard|daytime|ftp- data|ftp|telnet|smtp|time|hostname|whois|tacacs-ds |domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp-data |ftp|telnet|smtp|time|hostname|whois| tacacs-ds|domain |www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|dri p|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE]
	[sequence <1-2147483647>] permit udp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard| time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp| snmptrap|who|syslog|talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|time|nameserver|tacacs-ds |domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE]
	no sequence <1-2147483647>
Parameter	**<1-2147483647>:** (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.

	(A.B.C.D/A.B.C.D|any): Specify the source IPv4 address and mask of packet or any IPv4 address.
	(A.B.C.D/A.B.C.D|any): Specify the destination IPv4 address and mask of packet or any IPv4 address.
	[dscp VALUE]: (Optional) Specify the DSCP of packet.
	[precedence VLAUE]: (Optional) Specify the IP precedence of packet.
	icmp-type: Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
	icmp-code: Specify ICMP message code for filtering ICMP packet.
	l4-source-port: Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
	match-all: Specify tcp flag for TCP packet. If a flag should be set it is prefixed by\"+\".If a flag should be unset it is prefixed by\"-\".Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
Default	No default is defined.
Mode	IP ACL Configuration
Usage	Use the permit command to add permit conditions for an IP ACE that bypasses those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE.

Example:

The example shows how to add a set of ACEs. You can verify settings by the following show acl command.

This command shows how to permit a source IP address subnet.

```
Switch(config-ip-acl)# permit ip 192.168.1.0/255.255.255.0 any
```

This command shows how to permit ICMP echo-request packet with any IP address.

```
Switch(config-ip-acl)# permit icmp any any echo-request any
```

This command shows how to permit any IP address HTTP packets with DSCP 5.

```
Switch(config-ip-acl)# permit tcp any any any www dscp 5
```

This command shows how to permit any source IP address SNMP packet connect to destination IP address 192.168.1.1.

```
Switch(config-ip-acl)# permit udp any any 192.168.1.1/255.255.255.255 snmp
```

```
Switch(config-ip-acl)# show acl
IP access list iptest
sequence 1 permit ip 192.168.1.0/255.255.255.0 any
sequence 21 permit icmp any any echo-request any
sequence 41 permit tcp any any any www dscp 5
sequence 61 permit udp any any 192.168.1.1/255.255.255.255 snmp
```

2.6. deny (IP)

Item	Description
Syntax	[sequence <1-2147483647>] deny (<0- 255>|ipinip|egp|igp|hmp|rdp|ipv6| ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) [(dscp|precedence) VALUE]] [shutdown]
	[sequence <1-2147483647>] deny icmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (<0- 255>|echo-reply|destination-unreachable| source-quench|echo-request|router-advertisement|router- solicitation| time-exceeded|timestamp| timestamp-reply|traceroute|any) (<0-255>|any) [(dscp|precedence) VALUE] [shutdown]
	[sequence <1-2147483647>] deny tcp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo| discard|daytime|ftp- data|ftp|telnet|smtp|time|hostname|whois|tacacs-ds| domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip| PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet| smtp|time|hostname|whois|tacacs- ds|domain|www|pop2|pop3|syslog|talk| klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]
	[sequence <1-2147483647>] deny udp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|time|nameserver|tacacs- ds|domain|bootps| bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog| talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0- 65535>|echo| discard|time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp| sunrpc|ntp|netbios- ns|snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] [shutdown]
	no sequence <1-2147483647>
Parameter	**<1-2147483647>:** (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
	(A.B.C.D/A.B.C.D|any): Specify the source IPv4 address and mask of packet or any IPv4 address.

	(A.B.C.D/A.B.C.D|any): Specify the destination IPv4 address and mask of packet or any IPv4 address.
	[dscp VALUE]: (Optional) Specify the DSCP of packet.
	[precedence VLAUE]: (Optional) Specify the IP precedence of packet.
	icmp-type: Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
	icmp-code: Specify ICMP message code for filtering ICMP packet.
	l4-source-port: Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
	match-all: Specify tcp flag for TCP packet. If a flag should be set it is prefixed by\"+\".If a flag should be unset it is prefixed by\"-\".Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
	[shutdown]: (Optional) Shutdown interface while ACE hit
Default	No default is defined.
Mode	IP ACL Configuration
Usage	Use the deny command to add deny conditions for an IP ACE that drop those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. Use "**shutdown**" to shutdown interface while ACE hit.

Example:

The example shows how to add an ACE that denies packets with source IP address 192.168.1.80. You can verify settings by the following **show acl** command

```
Switch(config)# ip acl iptest
Switch(config-ip-acl)# deny ip 192.168.1.80/255.255.255.255 any
Switch(config-ip-acl)# show acl
IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```

2.7. ipv6 acl

Item	Description
Syntax	ipv6 acl NAME
	no ipv6 acl NAME
Parameter	**NAME:** Specify the name of IPv6 ACL

Default	No default is defined.
Mode	Global Configuration
Usage	Use the **ipv6 acl** command to create an IPv6 access list and to enter ipv6-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit “deny any” ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Example:

The example shows how to create an IPv6 ACL. You can verify settings by the following show acl command.

```
Switch(config)#ipv6 acl ipv6test
Switch(config-ipv6-acl)# show acl
  IPv6 access list iptest
```

2.8. permit (IPv6)

Item	Description
Syntax	[sequence <1-2147483647>] permit (<0-255>|ipv6) (X:X::X:X/<0-128>|any) (X:X::X:X/<0-128>|any) [(dscp|precedence) VALUE]
	[sequence <1-2147483647>] permit icmp (X:X::X:X/<0- 128>|any) (X:X::X:X/<0-128>|any) (<0-255>|destination- unreachable|packet-too-big| time-exceeded|parameter-problem|echo-request|echo-reply| mld-query|mld-report|mldv2-report|mld-done| router-solicitation|router-advertisement|nd-ns|nd-na|any) (<0-255>|any)[(dscp|precedence) VALUE]
	[sequence <1-2147483647>] permit tcp (X:X::X:X/<0- 128>|any) (<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp| time|hostname|whois|tacacs- ds|domain|www|pop2|pop3|syslog| talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-65535>|echo|discard|daytime|ftp- data|ftp| telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2| pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|an y) [match-all TCP_FLAG] [(dscp|precedence) VALUE]
	[sequence <1-2147483647>] permit udp (X:X::X:X/<0- 128>|any) (<0-65535>|echo|discard|time|nameserver|tacacs-ds|domain| bootps|bootpc|tftp|sunrpc|ntp|netbios- ns|snmp|snmptrap|who|syslog| talk|rip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-65535>|echo|discard|time|nameserver|tacacs-ds|domain|

	bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE]
	no sequence <1-2147483647>
Parameter	**<1-2147483647>:** (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
	(X:X::X:X/<0-128>|any): Specify the source IPv6 address and prefix of packet or any IPv6 address.
	(X:X::X:X/<0-128>|any): Specify the destination IPv6 address and prefix of packet or any IPv6 address.
	[dscp VALUE]: (Optional) Specify the DSCP of packet.
	[precedence VLAUE]: (Optional) Specify the IP precedence of packet.
	icmp-type: Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
	icmp-code: Specify ICMP message code for filtering ICMP packet.
	l4-source-port: Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
	match-all: Specify tcp flag for TCP packet. If a flag should be set it is prefixed by\"+\".If a flag should be unset it is prefixed by\"-\".Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
Default	No default is defined.
Mode	IPv6 ACL Configuration
Usage	Use the permit command to add permit conditions for an IPv6 ACE that bypasses those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE.

Example:

The example shows how to add a set of ACEs. You can verify settings by the following **show acl** command.

This command shows how to permit a source IP address subnet.

```
Switch(config-ipv6-acl)# permit ipv6 fe80:1122:3344:5566::1/64 any
Switch(config-ipv6-acl)# show acl
IPv6 access list ipv6test
sequence 1 permit ipv6 fe80:1122:3344:5566::1/64 any
```

2.9. deny (IPv6)

Item	Description
Syntax	sequence <1-2147483647>] deny (<0-255>|ipv6) (X:X::X:X/<0- 128>|any) (X:X::X:X/<0-128>|any) [(dscp|precedence) VALUE] [shutdown]
	[sequence <1-2147483647>] deny icmp (X:X::X:X/<0-128>|any) (X:X::X:X/<0-128>|any) (<0-255>|destination- unreachable|packet-too-big| time-exceeded|parameter-problem|echo-request|echo-reply| mld-query|mld-report|mldv2-report|mld-done| router-solicitation|router-advertisement|nd-ns|nd-na|any) (<0-255>|any)[(dscp|precedence) VALUE] [shutdown]
	[sequence <1-2147483647>] deny tcp (X:X::X:X/<0-128>|any) (<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp| time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog| talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-65535>|echo|discard|daytime|ftp- data|ftp| telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2| pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]
	[sequence <1-2147483647>] deny udp (X:X::X:X/<0-128>|any) (<0-65535>|echo|discard|time|nameserver|tacacs-ds|domain| bootps|bootpc|tftp|sunrpc|ntp|netbios- ns|snmp|snmptrap|who|syslog| talk|rip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-65535>|echo|discard|time|nameserver|tacacs-ds|domain| bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] [shutdown]
	no sequence <1-2147483647>
Parameter	**<1-2147483647>:** (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
	(A.B.C.D/A.B.C.D|any): Specify the source IPv4 address and mask of packet or any IPv4 address.
	(A.B.C.D/A.B.C.D|any): Specify the destination IPv4 address and mask of packet or any IPv4 address.
	[dscp VALUE]: (Optional) Specify the DSCP of packet.
	[precedence VLAUE]: (Optional) Specify the IP precedence of packet.
	icmp-type: Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
	icmp-code: Specify ICMP message code for filtering ICMP packet.
	l4-source-port: Specify TCP/UDP source port of for filtering TCP/UDP

	packet. Enter a port name of list or a number of TCP/UDP port.
	l4-destination-port: Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
	match-all: Specify tcp flag for TCP packet. If a flag should be set it is prefixed by\"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin,-urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
	[shutdown]: (Optional) Shutdown interface while ACE hit
Default	No default is defined.
Mode	IP ACL Configuration
Usage	Use the deny command to add deny conditions for an IPv6 ACE that drop those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. Use "**shutdown**" to shutdown interface while ACE hit.

Example:

The example shows how to add an ACE that denies packets with destination IP address fe80::abcd. You can verify settings by the following **show acl** command.

```
Switch(config)# ipv6 acl ipv6test
Switch(config-ipv6-acl)# deny ipv6 any fe80::abcd/128
Switch(config-ipv6-acl)# show acl
IPv6 access list ipv6test
sequence 1 deny ipv6 any fe80::abcd/128
```

2.10. show acl

Item	Description
Syntax	show acl
	show (mac|ip|ipv6) acl
	show (mac|ip|ipv6) acl NAME
Parameter	**(mac|ip|ipv6):** Specify a type of ACL to show
	NAME: Specify the name of ACL
Default	No default is defined.
Mode	Global Configuration. Context Configuration.

Usage	Use the **show acl** command to show created ACLs. You can specify mac、ip or ipv6 to show specific type ACL or specify unique name string to show ACL with the name.

Example:

The example shows how to show all IP ACL.

```
Switch# show ip acl
IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```

2.11. show acl utilization

Item	Description
Syntax	show acl utilization
Parameter	
Default	No default is defined.
Mode	Global Configuration
Usage	Use the **show acl utilization** command to show the usage of PIE of ASIC. When an ACL bind to interface, it needs ASIC resource to help to filter packet. An ASIC has limited resource. This command help user to know the PIE usage of AISC.

Example:

The example shows how to show utilization.

```
Switch# show acl utilization
Type: sys          usage: 128
Type: mac ACL      usage: 128
Type: IPv4 ACL     usage: 128
Type: IPv6 ACL     usage: 128
```

3. Administration

3.1. configure

Item	Description
Syntax	configure
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**configure**" command to enter global configuration mode. In global configuration mode, the prompt will show as "**Switch(config)#**".

Example:

This example shows how to enter global configuration mode.

```
Switch# configure
Switch(config)#
```

3.2. clear arp

Item	Description
Syntax	clear arp [A.B.C.D]
Parameter	**A.B.C.D** : Specify specific arp entry to clear.
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**clear arp**" command to clear all or specific one arp entry.

Example:

This example shows how to clear all arp entries.

```
Switch# clear arp
```

3.3. enable

Item	Description
Syntax	enable [<1-15>]
	disable [<1-14>]

Parameter	**<1-15>:** Specify privileged level to enable
	<1-14>: Specify privileged level to disable
Default	Default privilege level is 15 if no privilege level is specified on enable command. Default privilege level is 1 if no privilege level is specified on disable command.
Mode	User EXEC
Usage	In User EXEC mode, user only allows to do a few actions. Most of commands are only available in privileged EXEC mode. Use "**enable**" command to enter the privileged mode to do more actions on switch. In privileged EXEC mode, use "**exit**" command is able to go back to user EXEC mode with original user privilege level. If you need to go back to user EXEC mode with different privilege level, use "**disable**" command to specify the privilege level you need. In privileged EXEC mode, the prompt will show "Switch#"

Example:

This example shows how to enter privileged EXEC mode and show current privilege level.

```
Switch# exit
Switch> enable
Switch# show privilege
Current CLI Username:
Current CLI Privilege: 15
```

This example show how to enter user EXEC mode with privilege 3.

```
Switch# disable 3
Switch> show privilege
Current CLI Username:
Current CLI Privilege: 3
```

3.4. End

Item	Description
Syntax	end
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC Global Configuration Interface Configuration Line Configuration

	.....
Usage	Use “**end**” command to return to privileged EXEC mode directly. Every mode except User EXEC mode has the “end” command.

Example:

This example shows how to enter Interface Configuration mode and use end command to go back to privileged EXEC mode

```
Switch# configure Switch(config)# interface gi1
Switch(config-if)# end
Switch#
```

3.5. do

Item	Description
Syntax	do SEQUENCE
Parameter	**SEQUENCE**: Exec Command
Default	No default value for this command.
Mode	Privileged EXEC Global Configuration Interface Configuration Line Configuration .....
Usage	Use “**do**” command to run exec commands in current mode.

Example:

The example shows how to show ip

```
Switch(config-if)# do show ip
IP Address: 192.168.169.1
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.169.254
```

3.6. Exit

Item	Description
Syntax	exit
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC Global Configuration Interface Configuration

	Line Configuration
Usage	In User EXEC mode, "**exit**" command will close current CLI session. In othermodes, "**exit**" command will go to the parent mode. And every mode has the "**exit**" command.

Example:

This example shows how to enter privileged EXEC mode and use exit command to go back to user EXEC mode.

```
Switch> enable
Switch# exit
Switch>
```

3.7. History

Item	Description
Syntax	history <1-256>
	no history
Parameter	**<1-256>:** Specify maximum CLI history entry number.
Default	Default maximum history entry number is 128.
Mode	Line Configuration.
Usage	Use "history" command to specify the maximum commands history number for CLI running on console, telnet or ssh service. Every command input by user will record in history buffer. If all history commands exceed configured history number, older ones will be deleted from buffer. Use "no history" to disable the history feature. And use "show history" to show all history commands.

Example:

This example shows how to change console history number to 100, telnet history number to 150 and ssh history number to 200.

```
Switch(config)# line console
Switch(config-line)# history   100
Switch(config-line)# exit
Switch(config)# line telnet
 Switch(config-line)# history   150
Switch(config-line)# exit
Switch(config)# line ssh
 Switch(config-line)# history   200
Switch(config-line)# exit
```

This example shows how show line information.

```
Switch# show line
Console ==============================
    Session Timeout : 10 (minutes)
```

```
    History Count   : 100
    Password Retry  : 3
    Silent Time : 0 (seconds)
Telnet ================================
    Telnet Server   : disabled
    Session Timeout : 10 (minutes)
    History Count   : 150
    Password Retry  : 3
    Silent Time : 0 (seconds)
SSH ===================================
    SSH Server  : disabled
    Session Timeout : 10 (minutes)
    History Count   : 200
    Password Retry  : 3
    Silent Time : 0 (seconds)
```

This example shows how show history commands.

```
Switch# show history
Maximun History Count: 100
-------------------------------------------------
 1. configure
 2. interface gi1
 3. end
 4. show history
 5. show line
 6. configure
 7. line console
 8. history 100
 9. exit
 10. line telnet
 11. exit
 12. line telnet
 13. history
 14. exit
 15. line ssh
 16. exit
 17. line console
 18. end
 19. show line
 20. show history
```

3.8. Hostname

Item	Description
Syntax	hostname WORD
Parameter	WORD Specify the hostname of the switch.
Default	Default name string is “Switch”.
Mode	Global Configuration.

Usage	Use "**hostname**" command to modify hostname of the switch. The system name is also used to be CLI prompt.

Example:

This example shows how to modify contact information.

```
Switch(config)# hostname myname
myname(config)#
```

3.9. interface

Item	Description
Syntax	interface IF_PORTS
	interface range IF_PORTS
Parameter	**IF_PORTS:** Specify the port to select. This parameter allows partial port name and ignore case. For Example: gi1 GigabitEthernet4 ..... If port range is specified, the list format is also available. For Example:gi1-3 .....
Default	No default value for this command.
Mode	Global Configuration.
Usage	Some configurations are port based.Inorder to configure these configurations, we need to enter Interface Configuration mode to configure them. Use "**interface**" command to enter the Interface Configuration mode and select the port to be configured. In Interface Configuration mode, the prompt will show as "Switch(config-if)#"

Example:

This example shows how to enter Interface Configuration mode.

```
Switch# configure
Switch(config)# interface Gi1
Switch(config-if)#
```

3.10. ip address

Item	Description
Syntax	ip address A.B.C.D [mask A.B.C.D]

Parameter	**address A.B.C.D:** Specify IPv4 address for switch.
	mask A.B.C.D: Specify net mask address for switch
Default	Default IP address is 192.168.1.1 and default net mask is 255.255.255.0.
Mode	Global Configuration.
Usage	Use "**ip address**" command to modify administration ipv4 address. This address is very important. When we try to use telnet, ssh, http, https, snmp… to connect to the switch, we need to use this ip address to access it.

Example:

This example shows how to modify the ipv4 address of the switch.

```
Switch(config)# ip address 192.168.1.200 mask 255.255.255.0
```

This example shows how to show current ipv4 address of the switch.

```
Switch# show ip
IP Address: 192.168.1.200
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.254
```

3.11. ip default-gateway

Item	Description
Syntax	ip default-gateway A.B.C.D
	no ip default-gateway
Parameter	**A.B.C.D:** Specify default gateway IPv4 address for switch
Default	Default IP address of default gateway is 192.168.1.254.
Mode	Global Configuration.
Usage	Use "**ip default-gateway**" command to modify default gateway address. And use "**no ip default-gateway**" to restore default gateway address to factory default.

Example:

This example shows how to modify the ipv4 address of the switch.

```
Switch(config)# ip default-gateway 192.168.1.100
```

This example shows how to show current ipv4 default gateway of the switch.

```
Switch# show ip
IP Address: 192.168.1.1
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.100
```

3.12. ip dhcp

Item	Description
Syntax	ip dhcp
	no ip dhcp
Parameter	
Default	Default DHCP client is disabled.
Mode	Global Configuration.
Usage	Use "**ip dhcp**" command to enabled dhcp client to get IP address from remote DHCP server. Use "**no ip dhcp**" command to disabled dhcp client and use static ip address.

Example:

This example shows how to enable dhcp client.

```
Switch(config)# ip dhcp
```

This example shows how to show current dhcp client state of the switch.

```
Switch# show ip dhcp
 DHCP Status : enabled
```

3.13. ip dns

Item	Description
Syntax	ip dns *A.B.C.D* [*A.B.C.D*]
	ip dns X:X:XX:X:X [X:X::X:X]
	no ip dns [*A.B.C.D*]
	no ip dns X:X::X:X
Parameter	**A.B.C.D:** Specify the DNS server ip address.
	X:X:XX:X:X: IPV6 DNS server address.
Default	Default IP address of DNS server is 168.95.1.1 and 168.95.192.1.
Mode	Global Configuration.
Usage	Use "**ip dns**" command to modify DNS server address. And use "**no ip dns**"to delete existing DNS server.

Example:

This example shows how to modify the DNS server of the switch.

```
Switch(config)# ip dns 111.111.111.111 222.222.222.222
```

This example shows current DNS server of the switch.

```
Switch# show ip dns
DNS lookup is enabled
DNS Server 1 : 111.111.111.111
DNS Server 2 : 222.222.222.222
```

3.14. ip dns lookup

Item	Description
Syntax	ip dns lookup no ip dns lookup
Parameter	
Default	Default DNS lookup is enabled
Mode	Global Configuration.
Usage	Use "**ip dns lookup**" command to enable the Domain Name to IP address service. And use "no ip dns lookup" to disable the DNS service.

Example:

This example enables the DNS service on the system.

```
Switch(config)# ip dns lookup
```

This example shows the DNS service status.

```
Switch# show ip dns
DNS lookup is enabled
DNS Server 1 : 111.111.111.111
DNS Server 2 : 222.222.222.222
```

3.15. ipv6 autoconfig

Item	Description
Syntax	ipv6 autoconfig no ipv6 autoconfig
Parameter	
Default	Default IPv6 auto config is enabled.
Mode	Global Configuration.
Usage	Use "**ipv6 autoconfig**" command to enabled IPv6 auto configuration feature. Use "**no ipv6 autoconfig**" command to disabled IPv6 auto configuration feature.

Example:

This example shows how to disable IPv6 auto config.

```
Switch(config)# no ipv6 autoconfig
```

This example shows how to show current IPv6 auto config state.

```
Switch# show ipv6
IPv6 DHCP Configuration    : Disabled
IPv6 DHCP DUID     :
IPv6 Auto Configuration    : Disabled
IPv6 Link Local Address    : fe80::dcad:beff:feef:102/64
IPv6 static Address    : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address: fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::
```

3.16. ipv6 address

Item	Description
Syntax	ipv6 address X:X::X:X prefix <0-128>
Parameter	**address X:X::X:X:** Specify IPv6 address for switch.
	prefix <0-128>: Specify IPv6 prefix length for switch
Default	No default ipv6 address on the switch.
Mode	Global Configuration.
Usage	Use "**ipv6 address**" command to specify static IPv6 address.

Example:

This example shows how to add static ipv6 address of the switch.

```
Switch(config)# ipv6 address fe80::20e:2eff:fef1:4b3c prefix 128
```

This example shows how to show current ipv6 address of the switch.

```
Switch# show ipv6
IPv6 DHCP Configuration    : Disabled
IPv6 DHCP DUID     :
IPv6 Auto Configuration    : Enabled
IPv6 Link Local Address    : fe80::dcad:beff:feef:102/64
IPv6 static Address    : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address: fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::
```

3.17. ipv6 default-gateway

Item	Description
Syntax	ipv6 default-gateway X:X::X:X
Parameter	**X:X::X:X:** Specify default gateway IPv6 address for switch
Default	No default ipv6 default gateway address on the switch.
Mode	Global Configuration.
Usage	Use "**ipv6 default-gateway**" command to modify default gateway IPv6 address.

Example:

This example shows how to modify the ipv6 default gateway address of the switch.

```
Switch(config)# ipv6 default-gateway fe80::dcad:beff:feef:103
Switch# show ipv6
IPv6 DHCP Configuration    : Disabled
IPv6 DHCP DUID     :
IPv6 Auto Configuration    : Enabled
IPv6 Link Local Address    : fe80::dcad:beff:feef:102/64
IPv6 static Address    : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address: fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::
```

3.18. ipv6 dhcp

Item	Description
Syntax	ipv6 dhcp no ipv6 dhcp
Parameter	
Default	Default DHCPv6 client is disabled.
Mode	Global Configuration.
Usage	Use "**ipv6 dhcp**" command to enabled dhcpv6 client to get IP address from remote DHCPv6 server. Use "**no ipv6 dhcp**" command to disabled dhcpv6 client and use static ipv6 address or ipv6 auto config address.

Example:

This example shows how to enable dhcp client.

```
Switch(config)# ipv6 dhcp
```

This example shows how to show current dhcpv6 client state of the switch.

```
Switch# show ipv6 dhcp
DHCPv6 Status : enabled
```

3.19. ip service

Item	Description
Syntax	ip (telnet | ssh | http | https)
	no ip (telnet | ssh | http | https)
Parameter	**telnet**：Enable/Disable telnet service
	ssh: Enable/Disable ssh service
	http : Enable/Disable http service
	https: Enable/Disable https service
Default	Default telnet service is disabled. Default ssh service is disabled. Default http service is enabled. Default https service is disabled.
Mode	Global Configuration.
Usage	Use "**ip service**" command to enable all kinds of ip services. Such as telnet, ssh, http and https. Use no form to disable service.

Example:

This example shows how to enable telnet service and show current telnet service status.

```
Switch(config)# ip telnet Telnetd daemon enabled.
Switch(config)# exit
Switch# show line telnet
Telnet ==============================
    Telnet Server   : enabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 0 (seconds)
```

This example shows how to enable https service and show current https service status.

```
Switch(config)# ip https
Switch(config)# exit
Switch# show ip https
  HTTPS daemon : enabled
 Session Timeout : 10 (minutes)
```

3.20. ip session-timeout

Item	Description
Syntax	ip (http | https) session-timeout <0-86400>
Parameter	**http:** Specify session timeout for http service.
	https: Specify session timeout for https service.
	<0-86400>: Specify session timeout minutes. 0 means never timeout.
Default	Default session timeout for http and https is 10 minutes.
Mode	Global Configuration.
Usage	Use "**ip session-timeout**" command to specify the session timeout value for http or https service. When user login into WEBUI and do not do any action after session timeout will be logged out.

Example:

This example shows how to change http session timeout to 15min and https session timeout to 20min

```
Switch(config)# ip http session-timeout 15
Switch(config)# ip https session-timeout 20
```

This example shows how to enable https service and show current https service status.

```
Switch# show ip http
    HTTPS daemon : enabled
Session Timeout : 15 (minutes)
Switch# show ip https
    HTTPS daemon : disabled
 Session Timeout : 20 (minutes)
```

3.21. ip ssh

Item	Description
Syntax	ip ssh (v1|v2|all)
	no ip ssh (v1|v2|all)
Parameter	**v1:** Generate/Delete version 1 key files
	v2: Generate/Delete version 2 key files
	all: Generate/Delete version 1 and 2 key files
Default	Version 2 key files will be generated by default.
Mode	Global Configuration.
Usage	Use "ip ssh" command to generate the key files for ssh connection. Use no form to delete key files. SSH connection may not connect if no any v1 or v2 ssh key files exist.

Example:

This example shows how to delete and re-generate ssh version 2 key files.

```
Switch(config)# no ip ssh v2 Switch(config)# do show flash
File Name           File Size     Modified
--------------- ------------ --------------------------
 startup-config      2660       1970-01-01 00:00:46
 rsa2                1679       1970-01-01 00:00:23
 dsa2                672        1970-01-01 00:00:32
 ssl_cert            916        1970-01-01 00:00:39
 image0 (active)     8275248    2021-01-20 16:55:35
 image1 (backup)     0

Switch(config)# ip ssh v2
Generating a SSHv2 default RSA Key.
This may take a few minutes, depending on the key size.

Generating a SSHv2 default DSA Key.
This may take a few minutes, depending on the key size.

Switch(config)# do show flash
File Name            File Size      Modified
---------------- ------------ -------------------
startup-config       2660       1970-01-01 00:00:46
rsa2                 1679       1970-01-01 02:21:55
dsa2                 668        1970-01-01 02:22:02
ssl_cert             916        1970-01-01 00:00:39
image0 (active)      8275248    2021-01-20 16:55:35
image1 (backup)      0
```

3.22. Line

Item	Description
Syntax	line (console | telnet | ssh)
Parameter	**console**: Select console line to configure.
	telnet: Select telnet line to configure.
	ssh: Select ssh line to configure.
Default	No default value for this command.
Mode	Global Configuration.
Usage	Some configurations are line based. In order to configure these configurations,we need to enter Line Configuration mode to configure

	them. Use "**line**" command to enter the Line Configuration mode and select the line to be configured. In Line Configuration mode, the prompt will show as "Switch(config-line)#"

Example:

This example shows how to enter Interface Configuration mode

```
Switch# configure
Switch(config)# line console
Switch(config-line)#
```

3.23. Reboot

Item	Description
Syntax	reboot
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC.
Usage	Use "**reboot**" command to make system hot restart.

Example:

This example shows how to restart the system

```
Switch# reboot
```

3.24. enable password

Item	Description
Syntax	enable [privilege <1-15>] (password PASSWORD | secrect PASSWORD | secret encrypted PASSWORD)
	no enable [privilege <0-15>]
Parameter	**privilege <0-15>:** Specify the privilege level to configure. If no privilege level is specified, default is 15.
	password PASSWORD:Specify password string and make it not encrypted.
	secret PASSWORD：Specify password string and make it encrypted.
	secret encrypted PASSWORD: Enter an encrypted password. Use this keyword to enter a password that is already encrypted (for instance, a password that you copied from another the configuration file of

	another device).
Default	Default enable password for all privilege levels are “”.
Mode	Global Configuration.
Usage	Use “**enable password**” command to edit password for each privilege level for enable authentication. And use “**no enable**” command to restore enable password to default empty value. The only way to show this configuration is using “**Switch#show running-config**” command.

Example:

This example shows how to edit enable password for privilege level 15.

Specify password string and make it not encrypted.

```
Switch(config)# enable password admin
```

Specify password string and make it encrypted.

```
Switch(config)# enable secret admin
```

3.25. exec-timeout

Item	Description
Syntax	exec-timeout <0-65535>
Parameter	**<0-65535>:** Specify session timeout minutes. 0 means never timeout.
Default	Default session timeout for all lines are 10 minutes.
Mode	Global Configuration.
Usage	Use “**exec-timeout**” command to specify the session timeout value for CLI running on console, telnet or ssh service. When user login into CLI and do not do any action after session timeout will be logged out from the CLI session.

Example:

This example shows how to change console session timeout to 15min ,telnet session timeout to 20min and ssh session timeout to 25min.

```
Switch(config)# line console
Switch(config-line)# exec-timeout 15
Switch(config-line)# exit
Switch(config)# line telnet
Switch(config-line)# exec-timeout 20
Switch(config-line)# exit
```

```
Switch(config)# line ssh
Switch(config-line)# exec-timeout 25
Switch(config-line)# exit
```

This example shows how show line information.

```
Switch# show line
Console ==============================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 0 (seconds)
Telnet ===============================
    Telnet Server   : disabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 0 (seconds)
SSH ==================================
    SSH Server  : disabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 0 (seconds)
```

3.26. password-thresh

Item	Description
Syntax	password-thresh <0-120>
Parameter	**<0-120>:** Specify password fail retry number. 0 means no limit.
Default	Default password fail retry number is 3.
Mode	Line Configuration.
Usage	Use "**password-thresh**" command to specify the password fail retry number for CLI running on console, telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command "**silent-time**".

Example:

This example shows how to change console fail retry number to 4, telnet fail retry number to 5 and ssh fail retry number to 6.

```
Switch(config)# line console
Switch(config-line)# password-thresh 4
```

```
Switch(config-line)# exit
Switch(config)# line telnet
Switch(config-line)# password-thresh 5
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# password-thresh 6
Switch(config-line)# exit
```

This example shows how show line information.

```
Switch# show line
Console ==============================
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 4
    Silent Time : 0 (seconds)
Telnet ===============================
    Telnet Server   : disabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 5
    Silent Time : 0 (seconds)
SSH ==================================
    SSH Server  : disabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 6
    Silent Time : 0 (seconds)
```

3.27. ping

Item	Description
Syntax	ping HOSTNAME [count <1-999999999>]
Parameter	**HOSTNAME:** Specify IPv4/IPv6 address or domain name to ping.
	count <1-999999999>: Specify how many times to ping.
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**ping**" command to do network ping diagnostic.

Example:

This example shows how to ping remote host 192.168.1.111.

```
Switch# ping 192.168.1.111
```

```
PING 192.168.1.111 (192.168.1.111): 56 data bytes
64 bytes from 192.168.1.111: icmp_seq=0 ttl=128 time=10.0 ms
64 bytes from 192.168.1.111: icmp_seq=1 ttl=128 time=0.0 ms
64 bytes from 192.168.1.111: icmp_seq=2 ttl=128 time=0.0 ms
64 bytes from 192.168.1.111: icmp_seq=3 ttl=128 time=0.0 ms

--- 192.168.1.111 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
 round-trip min/avg/max = 0.0/2.5/10.0 ms
```

3.28. Traceroute

Item	Description
Syntax	traceroute HOSTNAME [max_hop <2-255>]
Parameter	**HOSTNAME:** Specify IPv4 to trace.
	max_hop <2-255>: Specify maximum hop to trace.
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**traceroute**" command to do network trace route diagnostic.

Example:

This example shows how to trace route host 192.168.1.111.

```
Switch# traceroute 192.168.1.111
traceroute to 192.168.1.111 (192.168.1.111), 30 hops max, 40 byte packets
  1 192.168.1.111 (192.168.1.111)  0 ms    10 ms   0 ms
```

3.29. show arp

Item	Description
Syntax	show arp
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "show arp" command to show all arp entries.

Example:

This example shows how to show arp entries.

```
Switch# show arp
Address         HWtype    HWaddress           Flags Mask       Iface
192.168.1.111   ether      00:0E:2E:F1:4B:3C        C          eth0
```

3.30. show cpu utilization

Item	Description
Syntax	show cpu utilization show cpu input rate
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show cpu utilization**" command to show current CPU utilization.

Example:

This example shows how to show current CPU utilization.

```
Switch# show cpu utilization
CPU utilization
---------------
 Current: 30%
```

3.31. show history

Item	Description
Syntax	show history
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC Global Configuration
Usage	Use "**show history**" to show commands we input before.

Example:

This example shows how show history commands.

```
Switch# show history
Maximun History Count: 128
------------------------------------------------------------
```

```
1. show line
2. config
3. line console
4. password-thresh 4
5. exit
6. line telnet
7. password-thresh 45
8. password-thresh 5
9. exit
10. line ssh
11. password-thresh 6
12. end
13. show line
14. ping 192.168.169.55
15. ping 192.168.169.55 4
16. ping 192.168.169.55 count 4
17. ping 192.168.169.56
18. traceroute 192.168.169.56
19. traceroute 192.168.169.1
20. show arp
21. show cpu utilization
22. show history
```

3.32. show info

Item	Description
Syntax	show info
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show info**" command to show system summary information.

Example:

This example shows how to show system version.

```
Switch# show info
System Name      : Switch
System Location  : Default
System Contact   : Default
MAC Address      : 00:E0:4C:00:00:00
IP Address       : 192.168.169.1
```

```
Subnet Mask      : 255.255.255.0
Loader Version   : 3.6.1.1
Loader Date      : Jan 20 2021 - 16:54:30
Firmware Version : 1.0.0x
Firmware Date    : Jan 20 2021 - 16:55:35
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time   : 0 days, 3 hours, 11 mins, 7 secs
```

3.33. show ip

Item	Description
Syntax	show ip
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ip**" command to show system IPv4 address, net mask and default gateway.

Example:

This example shows how to show current ipv4 address of the switch.

```
Switch# show ip
IP Address: 192.168.169.1
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.169.254
```

3.34. show ip dhcp

Item	Description
Syntax	show ip dhcp
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ip dhcp**" command to show IPv4 dhcp client enable state.

Example:

This example shows how to show current dhcp client state of the switch.

```
Switch# show ip dhcp
 DHCP Status : enabled
```

3.35. show ip dns

Item	Description
Syntax	show ip dns
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ip dns**" command to show system IPv4 DNS addresses.

Example:

This example shows how to show current ipv4 address of the switch.

```
Switch# show ip dns
DNS lookup is enabled
DNS Server 1 : 168.95.1.1
DNS Server 2 : 168.95.192.1
```

3.36. show ip http

Item	Description
Syntax	show ip (http|https)
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ip http**" command to show HTTP/HTTPS information.

Example:

This example shows how to show current ipv4 address of the switch.

```
Switch# show ip http
HTTP daemon : enabled
Session Timeout : 10 (minutes)

Switch# show ip https
HTTPS daemon : enabled
```

```
Session Timeout : 10 (minutes)
```

3.37. show ipv6

Item	Description
Syntax	show ipv6
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ipv6**" command to show system IPv6 address, net mask, default gateway and auto config state.

Example:

This example shows how to show current ipv6 address of the switch.

```
Switch# show ipv6
IPv6 DHCP Configuration     : Disabled
IPv6 DHCP DUID             :
IPv6 Auto Configuration     : Enabled
IPv6 Link Local Address     : fe80::2e0:4cff:fe00:0/64
IPv6 static Address         :
IPv6 static Gateway Address :
IPv6 in use Address         : fe80::2e0:4cff:fe00:0/64
```

3.38. show ipv6 mld snooping

Item	Description
Syntax	show ipv6 mld snooping
	show ipv6 mld snooping router [(dynamic|forbidden|static)]
	show ipv6 mld snooping groups [(dynamic|static)]
	show ipv6 mld snooping forward-all [vlan VLAN-LIST]
	show ipv6 mld snooping forward-all [vlan VLAN-LIST]
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ipv6 mld snooping**" command to show system IPv6 MLD snooping status and Packet Statistics.

Example:

This example shows how to display an IPv6 MLD snooping message for the current

switch.

```
Switch# show ipv6 mld snooping

                MLD Snooping Status
                --------------------

    Snooping                       : Disabled
    Report Suppression              : Enabled
    Operation Version               : v1
    Forward Method                  : mac
    Unknown IPv6 Multicast Action   : Flood


                Packet Statistics
    Total RX                        :  0
    Valid RX                        :  0
    Invalid RX                      :  0
    Other RX                        :  0
    Leave RX                        :  0
    Report RX                       :  0
    General Query RX                :  0
    Specail Group Query RX          :  0
    Specail Group & Source Query RX  :  0
    Leave TX                        :  0
    Report TX                       :  0
    General Query TX                :  0
    Specail Group Query TX          :  0
    Specail Group & Source Query TX  :  0
```

3.39. show ipv6 mld profile

Item	Description
Syntax	show ipv6 mld profile [<1-128>]
Parameter	**[<1-128>]:** MLD profile index.
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ipv6 mld profile**" command to show system IPv6 MLD profile configuration.

Example:

This example shows how to display an IPv6 MLD profile message for the current switch.

```
Switch# show ipv6 mld profile
MLD profile is empty
```

3.40. show ipv6 mld max-group

Item	Description
Syntax	show ipv6 mld max-group [interfaces IF_PORTS]
	show ipv6 mld max-group action [interfaces IF_PORTS]
Parameter	**interfaces IF_PORTS:** Specify port number
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use the "Show IPv6 MLD Max -group" command to display system IPv6 MLD Max group information and actions.

Example:

This example shows how to display an IPv6 MLD Max group message for the current switch.

```
Switch# show ipv6 mld max-group
Port ID  |  Max Group
---------+--------------
     gi1 : 256
     gi2 : 256
     gi3 : 256
     gi4 : 256
     gi5 : 256
     gi6 : 256
.................
Switch# show ipv6 mld max-group action
Port ID  |  Max-groups  Action
---------+---------------------
     gi1 : deny
     gi2 : deny
     gi3 : deny
     gi4 : deny
     gi5 : deny
     gi6 : deny
.................
```

3.41. show ipv6 mld filter

Item	Description
Syntax	show ipv6 mld filter [interfaces IF_PORTS]
Parameter	**interfaces IF_PORTS:** Specify port number
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use the command "Show IPv6 MLD Filter" to display the Profile ID for each port of the system IPv6 MLD.

Example:

This example shows how to display the IPv6 MLD Profile ID message for each port of the current swit.

```
Switch# show ipv6 mld filter
Port ID  |  Profile ID
---------+-------------
     gi1 : None
     gi2 : None
     gi3 : None
     gi4 : None
     gi5 : None
     gi6 : None
     gi7 : None
--More--
```

3.42. show ipv6 dhcp

Item	Description
Syntax	show ipv6 dhcp
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ipv6 dhcp**" command to show system IPv6 dhcp client enable state.

Example:

This example shows how to show current dhcpv6 client state of the switch.

```
Switch# show ipv6 dhcp
DHCPv6 Status : enabled
```

3.43. show line

Item	Description
Syntax	show line [(console | telnet | ssh)]
	clear line [(telnet | ssh)]
Parameter	**console:** Select console line to show.
	telnet: Select telnet line to show.
	ssh: Select ssh line to show.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show line**" command to show all line configurations including session timeout, history count, password retry number and silent time. For telnet and ssh, it also shows the service enable/disable state.

Example:

This example shows how show all lines' information.

```
Switch# show line
Console ==============================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 0 (seconds)
Telnet ===============================
    Telnet Server   : disabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 0 (seconds)
SSH ==================================
    SSH Server  : disabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 0 (seconds)
```

3.44. show memory statistics

Item	Description
Syntax	show memory statistics

Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show memory statistics**" command to show current memory utilization.

Example:

This example show how to show current system memory statistics.

```
Switch# show memory statistics
total(KB)   used(KB)    free(KB)    shared(KB)  buffer(KB)  cache(KB)
-----------+----------+-----------+---------+-----------+--------
Mem:    62408   56424       5984           0          1320    19328
-/+ buffers/cache: 35776   26632
Swap:   0   0   0
```

3.45. show privilege

Item	Description
Syntax	show privilege
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show privilege**" command to show the privilege level of the current user.

Example:

This example shows how to show arp entries.

```
Switch# show privilege
Current CLI Username:  admin
Current CLI Privilege: 15
```

3.46. show username

Item	Description
Syntax	show username
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC

Usage	Use "**show username**" command show all user accounts in local database.

Example:

This example shows how to show existing user accounts.

```
Switch# show username
Priv | Type |   User Name   |   Password
------+----+---------------+-----------------------
 01  | secret |             | dnXencJRwflV6
 15  | secret | admin       | FzjrGO6vfbERY
 15  | secret | test        | 7p57T9yMkViSUS
```

3.47. show users

Item	Description
Syntax	show users
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show users**" command show information of all active users.

Example:

This example shows how to show existing user accounts.

```
Switch# show users
Username          Protocol        Location
--------------- ------------ ----------------------
admin             console         0.0.0.0
admin             telnet       192.168.1.111
admin             ssh          192.168.1.111
```

3.48. show version

Item	Description
Syntax	show version
Parameter	
Default	No default value for this command.
Mode	User EXEC Privileged EXEC

Usage	Use "**show version**" command to show loader and firmware version and build date.

Example:

This example shows how to show system version.

```
Switch# show version
Loader Version   : 3.6.1.1
Loader Date      : Jan 20 2021 - 16:54:30
Firmware Version : 1.0.0x
Firmware Date    : Jan 20 2021 - 16:55:351
```

3.49. silent-time

Item	Description
Syntax	silent-time <0-65535>
Parameter	**<0-65535>:** Specify silent time with unit seconds. 0 means do not silent.
Default	Default silent time is 0.
Mode	Line Configuration
Usage	Use "**silent time**" command to specify the silent time for CLI running on console, telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command "**silent-time**".

Example:

This example shows how to change console silent time to 10, telnet silent time to 15 and ssh silent time to 20.

```
Switch(config)# line console
Switch(config-line)# silent-time 10
Switch(config-line)# exit
Switch(config)# line telnet
Switch(config-line)# silent-time 15
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# silent-time 20
Switch(config-line)# exit
```

This example shows how show line information.

```
Switch# show line
Console ==============================
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
```

```
    Silent Time : 10 (seconds)
Telnet ================================
    Telnet Server   : disabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 15  (seconds)
SSH ===================================
    SSH Server  : disabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time : 20 (seconds)
```

3.50. ssl

Item	Description
Syntax	ssl
Parameter	
Default	No default value for this command.
Mode	Global Configuration
Usage	Use "**ssl**" command to generate security certificate files such as RSA, DSA.

Example:

This example shows how to generate certificate files.

```
Switch# ssl
```

This example shows how to show the certificate file lists.

```
Switch# show flash
File Name                 File Size          Modified
------------------------ ---------------- ------------------------
 startup-config           2660             1970-01-01 00:00:46
 rsa2                     1679             1970-01-01 02:21:55
 dsa2                     668              1970-01-01 02:22:02
 ssl_cert                 916              1970-01-01 00:00:39
 image0 (active)          8275248          2021-01-20 16:55:35
 image1 (backup)          0
```

3.51. system name

Item	Description
Syntax	system name NAME
Parameter	**NAME:** Specify system name string.
Default	Default name string is “Switch”.
Mode	Global Configuration
Usage	Use “**system name**” command to modify system name information of the switch. The system name is also used to be CLI prompt.

Example:

This example shows how to modify contact information

```
Switch(config)# system name myname
myname(config)#
```

This example shows how to show system name information

```
Switch# show info
System Name      : myname
System Location  : Default
System Contact   : Default
MAC Address      : 00:E0:4C:00:00:00
IP Address       : 192.168.169.1
Subnet Mask      : 255.255.255.0
Loader Version   : 3.6.1.1
Loader Date      : Jan 20 2021 - 16:54:30
Firmware Version : 1.0.0x
Firmware Date    : Jan 20 2021 - 16:55:35
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time   : 0 days, 3 hours, 29 mins, 44 secs
```

3.52. system contact

Item	Description
Syntax	system contact CONTACT
Parameter	**CONTACT:** Specify contact string.
Default	Default contact string is “Default Contact”.
Mode	Global Configuration
Usage	Use “**system contact**” command to modify contact information of the switch.

Example:

This example shows how to modify contact information

```
Switch(config)# system contact callme
```

This example shows how to show system contact information

```
Switch# show info
System Name      : Switch
System Location  : Default
System Contact   : callme
MAC Address      : 00:E0:4C:00:00:00
IP Address       : 192.168.169.1
Subnet Mask      : 255.255.255.0
Loader Version   : 3.6.1.1
Loader Date      : Jan 20 2021 - 16:54:30
Firmware Version : 1.0.0x
Firmware Date    : Jan 20 2021 - 16:55:35
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time   : 0 days, 3 hours, 33 mins, 49 secs
```

3.53. system location

Item	Description
Syntax	system location LOCATION
Parameter	**CONTACT:** Specify location string.
Default	Default location string is “Default Location”.
Mode	Global Configuration
Usage	Use “**system location**” command to modify location information of the switch.

Example:

This example shows how to modify contact information

```
Switch(config)# system location home
```

This example shows how to show system location information

```
Switch# show info
System Name : Switch
System Location: home
System Contact   : callme
MAC Address      : 00:E0:4C:00:00:00
IP Address       : 192.168.169.1
Subnet Mask      : 255.255.255.0
Loader Version   : 3.6.1.1
```

```
Loader Date      : Jan 20 2021 - 16:54:30
Firmware Version : 1.0.0x
Firmware Date    : Jan 20 2021 - 16:55:35
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time   : 0 days, 3 hours, 33 mins, 49 secs
```

3.54. terminal length

Item	Description
Syntax	terminal length <0-24>
Parameter	**<0-24>:** Specify terminal length value. 0 means no limit.
Default	Default terminal length is 24.
Mode	User EXEC Privileged EXEC
Usage	Use "**terminal length**" command to specify the maximum line number the terminal is able to print.

Example:

This example shows how to change terminal length.

```
Switch# terminal length 3
Switch# show running-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: Switch TS928F Switch
! System Version: v1.0.0x
--More--
```

3.55. Username

Item	Description
Syntax	username WORD<0-32> [privilege (admin|user|<0-15>)] (nopassword | password UNENCRYPY-PASSWORD | secrect UNENCRYPY-PASSWORD | secret encrypted ENCRYPT-PASSWORD)
	no username WORD<0-32>
Parameter	**username WORD<0-32>:** Specify user name to add/delete/edit.
	privilege admin: Specify privilege level to be admin (privilege 15)
	privilege user: Specify privilege level to be user (privilege 1)
	privilege <0-15>: Specify custom privilege level
	password UNENCRYPY- PASSWORD: Specify password string and make it not encrypted.
	secret UNENCRYPY- PASSWORD: Specify password string and make it

	encrypted.
	secret encrypted ENCRYPT- PASSWORD: Enter an encrypted password. Use this keyword to enter a password that is already encrypted (for instance, a password that you copied from another the configuration file of another device).
Default	Default username “admin” has password “admin” with privilege 15.
Mode	Global Configuration
Usage	Use “**username**” command to add a new user account or edit an existing user account. And use “**no username**” to delete an existing user account. The user account is a local database for login authentication.

Example:

This example shows how to add a new user account.

```
Switch(config)# username test secret passwd
```

This example shows how to show existing user accounts.

```
Switch# show username
Priv | Type |   User Name   |   Password
-----+------+-----------+-----------------------
  15| secret |   admin | MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM=
  15| secret |    test | NzZhMjE3M2JlNjM5MzI1NGU3MmZmYTRkNmRmMTAzMGE=
```

4. Authentication Manager

4.1. authentication

Item	Description
Syntax	authentication (dot1x|mac|web)
	no authentication (dot1x|mac|web)
Parameter	
Default	Default is disabled for all type
Mode	Global Configuration
Usage	Use "**authentication**" command to enable the global setting of 802.1x/MAC/WEB authentication network access control. Use the no form of this command to disable 802.1x/MAC/WEB authentication.

Example:

The following example shows how to enable 802.1x/MAC/WEB authentication.

```
Switch(config)# authentication dot1x
Switch(config)# authentication mac
Switch(config)# authentication web
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                      : disabled
Mac-auth Radius User ID Format: XXXXXXXXXXXX

.....
```

4.2. authentication (Interface)

Item	Description
Syntax	authentication **(**dot1x|mac|web**)**
	no authentication (dot1x|mac|web)
Parameter	
Default	Default is disabled for all type
Mode	Interface Configuration
Usage	Use "**authentication**" interface command to enable the port setting of 802.1x/MAC/WEB authentication network access control.

	Use the no form of this command to disable 802.1x/MAC/WEB authentication.

Example:

The following example shows how to enable 802.1x/MAC/WEB authentication.

```
Switch(config)#interface Gi1
Switch(config-if)# authentication dot1x
Switch(config-if)# authentication mac
Switch(config-if)# authentication web
Switch# show authentication interface Gi1
Interface GigabitEthernet1
Admin Control   : disable
Host Mode   : multi-auth
Type dot1x State    : enabled
Type mac State  : enabled
Type web State  : enabled
……
```

4.3. authentication guest-vlan

Item	Description
Syntax	authentication guest-vlan <1-4094>
	no authentication guest-vlan
Parameter	**<1-4094>:** Guest VLAN ID
Default	Default guest VLAN is disabled
Mode	Global Configuration
Usage	Use "**authentication guest-vlan**" command to enable the global setting of guest VLAN and specify guest VLAN ID. Use the no form of this command to disable guest VLAN.

Example:

The following example shows how to create guest VLAN.

```
Switch(config)# vlan 3
Switch(config-vlan)# exit
Switch(config)# authentication guest-vlan 3
Switch# show authentication
Autentication dot1x state  : enabled
Autentication mac state    : disabled
Autentication web state    : disabled
Guest VLAN  : enabled (3)
Mac-auth Radius User ID Format: XXXXXXXXXXXX
```

.....

4.4. authentication guest-vlan (Interface)

Item	Description
Syntax	authentication guest-vlan
	no authentication guest-vlan
Parameter	
Default	Default guest VLAN is disabled
Mode	Interface Configuration
Usage	Use "**authentication guest-vlan**" command to enable the port setting of guest VLAN. Use the no form of this command to disable guest VLAN.

Example:

The following example shows how to enable guest VLAN.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication guest-vlan
Switch# show authentication
Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : enabled
  Reauthentication       : disabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
```

4.5. authentication host-mode

Item	Description
Syntax	authentication host-mode (multi-auth|multi-host|single-host)
	no authentication host-mode
Parameter	**multi-auth:** Multiple Authentication Mode. In this mode, every client need to pass authenticate procedure individually.
	multi-host: Multiple Host Mode. In this mode, only one client need to be

	authenticated and other clients will get the same access accessibility.
	single-host: Single Host Mode. In this mode, only one host is allowed to be authenticated. It is the same as multi-auth mode with max hosts number configure to be 1.
Default	Default is multi-auth mode.
Mode	Interface Configuration
Usage	Use "**authentication host-mode**" command to configure the port authentication host mode. Use the **no** form of this command to restore default value.

Example:

The following example shows how to modify port host mode to multi-host.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication host-mode multi-host
Switch# show authentication interface Gi1
Interface GigabitEthernet1
   Admin Control          : disable
   Host Mode              : multi-host
   Type dot1x State       : disabled
   Type mac State         : disabled
   Type web State         : disabled
  ……
```

4.6. authentication max-hosts

Item	Description
Syntax	authentication max-hosts <1-256>
	no authentication max-hosts
Parameter	**<1-256>:** Available max host number in multi-auth mode.
Default	Default max host number is 256
Mode	Interface Configuration
Usage	Use "**authentication max-hosts**" command to configure the port max hosts number for multi-auth mode. The host exceed the max host number is not allowed to create authentication session and do authenticating. Use **no** form of this command to restore default value.

Example:

The following example shows how to change port max hosts number.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication max-hosts 100
Switch# show authentication interface Gi1
```

```
Interface GigabitEthernet1
Admin Control   : disable
Host Mode   : multi-auth
Type dot1x State    : disabled
Type mac State  : disabled
Type web State  : disabled
Type Order  : dot1x
MAC/WEB Method Order    : radius
Guest VLAN  : disabled
Reauthentication    : disabled
Max Hosts   : 100
  ……
```

4.7. authentication method

Item	Description
Syntax	authentication method (local [radius] | radius [local])
	no authentication method
Parameter	**local:** Use local account to authenticate
	radius: Use remote RADIUS server to authenticate
Default	Default is RADIUS method in first place and no other method.
Mode	Interface Configuration
Usage	Use "**authentication method**" command to configure the port authentication method order. Use the **no** form of this command to restore default value.

Example:

The following example shows how to modify port authentication order to local and then RADIUS.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication method local radius
Switch# show authentication interface Gi1
Interface GigabitEthernet1
Admin Control   : auto
Host Mode   : multi-host
Type dot1x State    : disabled
Type mac State  : disabled
Type web State  : disabled
Type Order      : dot1x mac web
MAC/WEB Method Order    : local radius
……
```

4.8. authentication order

Item	Description
Syntax	authentication order (dot1x [mac] [web] | mac [dot1x] [web] | web)
	no authentication order
Parameter	**dot1x**：Authenticating user by IEEE 802.1X
	mac：Authenticating user by mac based authentication
	web: Authenticating user by web based authentication
Default	Default is dot1x type in first place and no other types.
Mode	Interface Configuration
Usage	Use "**authentication order**" command to configure the port authentication type order. Use the **no** form of this command to restore default value

Example:

The following example shows how to modify port authentication order to dot1x, mac and web.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication order dot1x mac web
Switch# show authentication interface Gi1
Interface GigabitEthernet1
Admin Control   : auto
Host Mode   : multi-host
Type dot1x State    : disabled
Type mac State  : disabled
Type web State  : disabled
Type Order  : dot1x mac web
.....
```

4.9. authentication port-control

Item	Description
Syntax	authentication port-control (auto|force-auth|force-unauth)
	no authentication port-control
Parameter	**auto:** Need passing authentication procedure to get network accessibility
	Force-auth: Port is force authorized and all clients have network accessibility.
	force-unauth: Port is force unauthorized and all clients have no network accessibility.

Default	Default is disabled.
Mode	Interface Configuration
Usage	Use "**authentication port-control**" command to enable the port authentication control mode. Use the **no** form of this command to disable authentication port control.

Example:

The following example shows how to configure port control to auto mode.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication port-control auto
Switch# show authentication interface Gi1
Interface GigabitEthernet1
Admin Control   : auto
Host Mode   : multi-auth
Type dot1x State    : disabled
Type mac State  : disabled
Type web State  : disabled
.....
```

4.10. authentication radius-attributes vlan

Item	Description
Syntax	authentication radius-attributes vlan (reject | static)
	no authentication radius-attributes vlan
Parameter	**reject:** If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized.
	static: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.
Default	Default radius attributes VLAN assign mode is static.
Mode	Interface Configuration
Usage	Use "**authentication radius-attributes vlan**" command to configure the port RADIUS VLAN assign mode. Use the **no** form of this command to disable the port RADIUS VLAN assign.

Example:

The following example shows how to configure port VLAN assign to reject mode.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication radius-attributes vlan reject
Switch# show authentication interface Gi1
```

```
Interface GigabitEthernet1
Admin Control   : disable
Host Mode   : multi-auth
Type dot1x State    : disabled
Type mac State  : disabled
Type web State  : disabled
Type Order  : dot1x
MAC/WEB Method Order    : radius
Guest VLAN  : disabled
Reauthentication    : disabled
Max Hosts   : 256
VLAN Assign Mode    : reject
……
```

4.11. authentication reauth

Item	Description
Syntax	authentication reauth no authentication reauth
Parameter	
Default	Default is disabled.
Mode	Interface Configuration
Usage	Use "**authentication reauth**" command to enable the port reauthentication. Use the **no** form of this command to disable reauthentication.

Example:

The following example shows how to enable port reauthentication.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication reauth
Switch# show authentication interface Gi1
Interface GigabitEthernet1
Admin Control   : disable
Host Mode   : multi-auth
Type dot1x State    : disabled
Type mac State  : disabled
Type web State  : disabled
Type Order  : dot1x
MAC/WEB Method Order    : radius
Guest VLAN  : disabled
Reauthentication    : enabled
……
```

4.12. authentication timer inactive

Item	Description
Syntax	authentication timer inactive <60-65535>
	no authentication timer inactive
Parameter	**<60-65535>:** Interval in seconds after which if there is no activity from the client then it will be unauthorized.
Default	Default inactive timeout is 60 seconds.
Mode	Interface Configuration
Usage	Use "**authentication timer inactive**" command to configure the port inactive timeout value. Sometimes, we may assign a long aging time for a host, but in fact, it is not active. This inactive timeout will detect the host is active or not. If the host is inactive exceed this timeout, it should be removed. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port inactive period.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication timer inactive 300
Switch# show authentication interface Gi1
Interface GigabitEthernet1
……
Common Timers
    Reauthenticate Period: 300
    Inactive Timeout : 300
    Quiet Period : 60
802.1x Parameters
    EAP Max Request: 2
    EAP TX Period : 30
    Supplicant Timeout : 30
    Server Timeout : 30
Web-auth Parameters
    Login Attempt : 3
```

4.13. authentication timer quiet

Item	Description
Syntax	authentication timer quiet <0-65535>
	no authentication timer quiet

Parameter	**<0-65535>:** Interval in seconds to wait following a failed authentication exchange
Default	Default quiet period is 60 seconds
Mode	Interface Configuration
Usage	Use "**authentication timer quiet**" command to configure the port quiet period value. After authenticating fail many times and the port is guest VLAN disabled, the port/host will enter lock state until quiet period expired. In lock state, the port/host is not allowed to do authenticating. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port quiet period.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication timer quiet 300
Switch# show authentication interface Gi1
Interface GigabitEthernet1
.....
Common Timers
    Reauthenticate Period: 300
    Inactive Timeout : 300
    Quiet Period : 300
802.1x Parameters
    EAP Max Request: 2
    EAP TX Period : 30
    Supplicant Timeout : 30
    Server Timeout : 30
Web-auth Parameters
    Login Attempt : 3
```

4.14. authentication timer reauth

Item	Description
Syntax	authentication timer reauth <300-4294967294>
	no authentication timer reauth
Parameter	**<300-4294967294>:** Time in seconds after which an automatic reauthentication should be initiated.
Default	Default reauthentication period is 3600 seconds.
Mode	Interface Configuration
Usage	Use "**authentication timer reauth**" command to configure the port reauthentication period value with unit second if the reauthentication time is

	not assigned by local database or remote authentication server. On the other hand, if the reauthentication time is assigned by local database or remote server, this configured reauthentication time will be ignored. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port reauthentication period.

```
Switch(config)# interface Gi1
Switch(config-if)# authentication timer reauth 300
Switch# show authentication interface Gi1
Interface GigabitEthernet1
……
Common Timers
    Reauthenticate Period: 300
    Inactive Timeout   : 60
    Quiet Period   : 60
802.1x Parameters
    EAP Max Request: 2
    EAP TX Period : 30
    Supplicant Timeout : 30
    Server Timeout : 30
Web-auth Parameters
    Login Attempt : 3
```

4.15. authentication mac radius

Item	Description
Syntax	authentication mac radius mac-delimiter (colon|dot|hyphen|none) [gap (2|4|6)]
	authentication mac radius mac-case (lower|upper)
Parameter	**colon**:Use ':' as delimiter
	dot:Use '.' as delimiter
	hyphen: Use '-' as delimiter
	none: No delimiter
	[gap (2|4|6)]: The gap of each delimiter
	lowe: Use lower case
	upper: Use upper case
Default	
Mode	Global Configuration
Usage	Use "**authentication mac radius mac-****" command to configure authentication manager mac-auth radius user id format.

Example:

The following example shows how to configure authentication manager mac-auth radius user id format.

```
Switch(config)# authentication mac radius mac-delimiter colon gap 2
Switch(config)# authentication mac radius mac-case lower
```

4.16. authentication mac local

Item	Description
Syntax	authentication mac local A:B:C:D:E:F control auth [vlan <1-4094>] [reauth-period <300-4294967294>] [inactive-timeout <60-65535>]
	authentication mac local A:B:C:D:E:F control unauth
	no authentication mac local A:B:C:D:E:F
Parameter	**A:B:C:D:E:F**:MAC address of entry to be added
	[vlan <1-4094>]: Local entry assigned vlan
	[reauth-period <300-4294967294>]:Time in seconds after which an automatic re-authentication should be initiated
	[inactive-timeout <60-65535>]:Interval in seconds after which if there is no activity from the client then it will be unauthorized
Default	
Mode	Global Configuration
Usage	Use "**authentication mac local****" command to set macauth authentication local database. Use the **no** form of this command to restore the delay to default value.

Example:

The following example shows how to configure macauth authentication local database.

```
Switch(config)# authentication mac local 00:11:22:33:44:55 control auth vlan 22 inactive-timeout 60
```

4.17. authentication web local username

Item	Description
Syntax	authentication web local username WORD<1-32> password [encrypted] PASSWORD [vlan <1-4094>] [reauth-period <300-4294967294>] [inactive-timeout <60-65535>]
	no authentication web local username WORD<1-32>
Parameter	**WORD<1-32>**:Specify user name to be added
	PASSWORD: Specify password of the user
	[vlan <1-4094>]:Local entry assigned vlan
	[reauth-period <300-4294967294>]:Time in seconds after which an automatic re-authentication should be initiated
	[inactive-timeout <60-65535>]:Interval in seconds after which if there is no activity from the client then it will be unauthorized

Default	
Mode	Global Configuration
Usage	Use "**authentication web local username****" command to set web authentication local database Use the **no** form of this command to restore the delay to default value.

Example:

The following example shows how to configure macauth authentication local database.

```
Switch(config)# authentication web local username admin password admin vlan 1 inactive-timeout 60
```

4.18. authentication web max-login-attempts

Item	Description
Syntax	authentication web max-login-attempts (infinite|<3-10>)
	no authentication web max-login-attempts
Parameter	**infinite**:No limit to login attempt number
	<3-10>: Maximum number of allowed login attempts on the interface
Default	Default login attempt is 3.
Mode	Interface Configuration
Usage	Use "**authentication web max-login-attempts**" command to set max web auth login attempt number. Use the **no** form of this command to restore the delay to default value.

Example:

The following example shows how to configure max web auth login attempt number.

```
Switch(config-if)# authentication web max-login-attempts 4
```

4.19. clear authentication sessions

Item	Description
Syntax	clear authentication sessions
	clear authentication sessions interfaces IF_NMLPORTS
	clear authentication sessions mac mac-addr
	clear authentication sessions session-id WORD
	clear authentication sessions type (dot1x|mac|web)
Parameter	**interfaces IF_NMLPORTS:** Clear sessions on specific interface
	mac mac-addr: Clear session with specific MAC address
	session-id WORD: Clear session with specific session ID
	type(dot1x|mac|web): Clear session with specific authentication type
Default	Default is no local authentication entry.

Mode	Privileged EXEC
Usage	Use "**clear authentication sessions**" command to delete existing authentication sessions. If no parameter is specified, all sessions will be deleted. After authentication session is deleted, host need to do authentication procedure again.

Example:

The following example shows how to clear all authentication sessions.

```
Switch# clear authentication sessions
Switch# show authentication sessions
 No Auth Manager sessions currently exist
```

4.20. dot1x

Item	Description
Syntax	dot1x
	no dot1x
Parameter	
Default	Default 802.1x is disabled
Mode	Global Configuration
Usage	Use "**dot1x**" command to enable the global setting of 802.1x. The "**authentication dot1x**" command has the same effect as this one. This command is a backward compatible command. Use the **no** form of this command to disable 802.1x authentication.

Example:

The following example shows how to enable 802.1x authentication.

```
Switch(config)# dot1x
Switch# show authentication
Autentication dot1x state  : enabled
Autentication mac state    : disabled
Autentication web state    : disabled
Guest VLAN  : enabled (3)
Mac-auth Radius User ID Format: XXXXXXXXXXXX

……
```

4.21. dot1x guest-vlan

Item	Description
Syntax	dot1x guest-vlan <1-4094>
	no dot1x guest-vlan
Parameter	**<1-4094>:** Guest VLAN ID
Default	Default guest VLAN is disabled
Mode	Global Configuration
Usage	Use "**dot1x guest-vlan**" command to enable the global setting of guest VLAN and specify guest VLAN ID. Use the **no** form of this command to disable guest VLAN.

Example:

The following example shows how to create guest VLAN.

```
Switch(config)# vlan 3
Switch(config-vlan)# exit
Switch(config)# dot1x guest-vlan 3
Switch# show authentication
Autentication dot1x state  : enabled
Autentication mac state    : disabled
Autentication web state    : disabled
Guest VLAN  : enabled (3)
Mac-auth Radius User ID Format: XXXXXXXXXXXX
```

4.22. dot1x max-req

Item	Description
Syntax	dot1x max-req <1-10>
	no dot1x max-req
Parameter	**<1-10>:** The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout),the authentication process is restarted.
Default	Default EAP max request number is 2.
Mode	Interface Configuration
Usage	Use "**dot1x max-req**" command to configure the port 802.1x max EAP request value. The max request is the maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port 802.1x EAP TX period.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x max-req 1
Switch# show authentication interface Gi1
Interface GigabitEthernet1
……
Common Timers
Reauthenticate Period: 300
Inactive Timeout : 300
Quiet Period : 300
802.1x Parameters
EAP Max Request: 1
EAP TX Period  : 10
Supplicant Timeout : 120
Server Timeout : 150
Web-auth Parameters
Login Attempt  : 3
```

4.23. dot1x port-control

Item	Description
Syntax	dot1x port-control (auto|force-auth|force-unauth)
	no dot1x port-control
Parameter	**auto:** Need passing authentication procedure to get network accessibility
	force-auth: Port is force authorized and all clients have network accessibility.
	force-unauth: Port is force unauthorized and all clients have no network accessibility.
Default	Default is disabled.
Mode	Interface Configuration
Usage	Use "**dot1x port-control**" command to enable the port authentication control mode. The "**authentication port-control**" command has the same effect. Use the **no** form of this command to disable authentication port control.

Example:

The following example shows how to configure port control to auto mode.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x port-control auto
Switch# show authentication interface Gi1
```

```
Interface GigabitEthernet1
Admin Control   : auto
Host Mode   : multi-auth
Type dot1x State    : enabled
Type mac State  : disabled
Type web State  : disabled
……
```

4.24. dot1x reauth

Item	Description
Syntax	dot1x reauth
	no dot1x reauth
Parameter	
Default	Default is disabled.
Mode	Interface Configuration
Usage	Use "**dot1x reauth**" command to enable the port reauthentication. The "**authentication reauth**" command has the same effect, it is a backward compatible command Use the **no** form of this command to disable reauthentication.

Example:

The following example shows how to enable port reauthentication.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x reauth
Switch# show authentication interface Gi1
Interface GigabitEthernet1
Admin Control   : disable
Host Mode   : multi-auth
Type dot1x State    : disabled
Type mac State  : disabled
Type web State  : disabled
Type Order  : dot1x
MAC/WEB Method Order    : radius
Guest VLAN  : disabled
Reauthentication    : enabled
……
```

4.25. dot1x timeout reauth-period

Item	Description
Syntax	dot1x timeout reauth-period <300-4294967294>
	no dot1x timeout reauth-period
Parameter	**<300-4294967294>:** Time in seconds after which an automatic reauthentication should be initiated
Default	Default reauthentication period is 3600 seconds.
Mode	Interface Configuration
Usage	Use "**dot1x timout reauth**" command to configure the port reauthentication period value with unit second if the reauthentication time is not assigned by local database or remote authentication server. On the other hand, if the reauthentication time is assigned by local database or remote server, this configured reauthentication time will be ignored. The "**authentication timer reauth**" command has the same effect and it is a backward compatible command. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port 802.1x reauthentication period.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x timeout reauth-period 300
Switch# show authentication interface Gi1
Interface GigabitEthernet1
……
Common Timers
Reauthenticate Period: 300
Inactive Timeout   : 60
Quiet Period   : 60
802.1x Parameters
EAP Max Request: 2
EAP TX Period : 30
Supplicant Timeout : 30
Server Timeout : 30
Web-auth Parameters
Login Attempt : 3
```

4.26. dot1x timeout quiet-period

Item	Description
Syntax	dot1x timeout quiet-period <0-65535>
	no dot1x timeout quiet-period
Parameter	**<0-65535>:** Interval in seconds to wait following a failed authentication exchange
Default	Default quiet period is 60 seconds.
Mode	Interface Configuration
Usage	Use "**dot1x timeout quiet-period**" command to configure the port quiet period value. The "**authentication timer quiet**" command has the same effect and it is backward compatible command. After authenticating fail many times and the port is guest VLAN disabled, the port/host will enter lock state until quiet period expired. In lock state, the port/host is not allowed to do authenticating. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port 802.1x quiet period.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x timeout quiet-period 300
Switch# show authentication interface Gi1
Interface GigabitEthernet1
……
Common Timers
Reauthenticate Period: 300
Inactive Timeout : 300
Quiet Period : 300
802.1x Parameters
EAP Max Request: 2
EAP TX Period : 30
Supplicant Timeout : 30
Server Timeout : 30
Web-auth Parameters
Login Attempt : 3
```

4.27. dot1x timeout server-timeout

Item	Description
Syntax	dot1x timeout server-timeout <1-65535>
	no dot1x timeout server-timeout

Parameter	**<1-65535>:** Number of seconds that lapses before the device resends a request to the authentication server.
Default	Default server timeout is 30 seconds.
Mode	Interface Configuration
Usage	Use "**dot1x timeout server-timeout**" command to configure the port 802.1x server timeout value. The server timeout is the number of seconds that lapses before the device resends a request to the authentication server. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port 802.1x server timeout.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x timeout server-timeout 150
Switch# show authentication interface Gi1
Interface GigabitEthernet1
.....
Common Timers
Reauthenticate Period: 300
Inactive Timeout : 300
Quiet Period : 300
802.1x Parameters
EAP Max Request: 2
EAP TX Period  : 30
Supplicant Timeout : 120
Server Timeout : 150
Web-auth Parameters
Login Attempt  : 3
```

4.28. dot1x timeout supp-timeout

Item	Description
Syntax	dot1x timeout supp-timeout <1-65535>
	no dot1x timeout supp-timeout
Parameter	**<1-65535>:** Number of seconds that lapses before EAP requests are resent to the supplicant
Default	Default supplicant timeout is 30 seconds.
Mode	Interface Configuration
Usage	Use "**dot1x timeout supp-timeout**" command to configure the port supplicant timeout value. The supplicant timeout is the number of seconds that lapses before EAP requests are resent to the supplicant. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port 802.1x supplicant timeout.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x timeout supp-timeout 120
Switch# show authentication interface Gi1
Interface GigabitEthernet1
.....
Common Timers
Reauthenticate Period: 300
Inactive Timeout : 300
Quiet Period : 300
802.1x Parameters
EAP Max Request: 2
EAP TX Period  : 30
Supplicant Timeout : 120
Server Timeout : 30
Web-auth Parameters
Login Attempt  : 3
```

4.29. dot1x timeout tx-period

Item	Description
Syntax	dot1x timeout tx-period <1-65535>
	no dot1x timeout tx-period
Parameter	**<1-65535>:** Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
Default	Default EAP TX period is 30 seconds.
Mode	Interface Configuration
Usage	Use "**dot1x timeout tx-period**" command to configure the port 802.1x EAP TX period value. The TX period is the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request. Use **no** form of this command to restore default value.

Example:

The following example shows how to configure port 802.1x EAP TX period.

```
Switch(config)# interface Gi1
Switch(config-if)# dot1x timeout tx-period 10
Switch# show authentication interface Gi1
```

```
Interface GigabitEthernet1
……
Common Timers
Reauthenticate Period: 300
Inactive Timeout : 300
Quiet Period : 300
802.1x Parameters
EAP Max Request: 2
EAP TX Period  : 10
Supplicant Timeout : 120
Server Timeout : 150
Web-auth Parameters
Login Attempt  : 3
```

4.30. show authentication

Item	Description
Syntax	show authentication
	show authentication interfaces IF_PORTS
Parameter	**interfaces IF_PORTS** : Specify port list to show port configurations.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show authentication**" command to show all authentication manager configurations. Use "**show authentication interface**" command to show authentication manager configuration of specific port.

Example:

This example shows how to show the mac authentication configurations of port gi1.

```
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : disabled
Autentication web state       : disabled
Guest VLAN                   : enabled (3)
Mac-auth Radius User ID Format: XXXXXXXXXXXX
Mac-auth Local Entry          :
Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
```

```
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 450
    Inactive Timeout     : 300
    Quiet Period         : 456
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 123
    Supplicant Timeout   : 111
    Server Timeout       : 30
  Web-auth Parameters
    Login Attempt        : 3
……
Switch# show authentication interface Gi7
Interface Configurations

Interface GigabitEthernet7
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
```

```
  Server Timeout       : 30
Web-auth Parameters
  Login Attempt        : 3
```

4.31. show authentication sessions

Item	Description
Syntax	show authentication sessions [detail]
	show authentication sessions interface IF_PORTS
	show authentication sessions session-id WORD
	show authentication session type (dot1x|mac|web)
Parameter	**detail:** Show session detail information.
	interface IF_PORTS: Show session detail information of specific port.
	session-id WORD: Show session detail information of specific session id
	type (dot1x|mac|web): Show session detail information of specific authentication type
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show authentication sessions**" command to show authentication detail session information.

Example:

This example shows how to show current authentication session brief and detail information.

```
Switch# show authentication sessions
Interface   MAC Address Type    Status      Session     ID
---------- ----------------- -------- ------------ ----------------
 gi7        00:01:6C:CB:29:4A  dot1x     Authorized    000000010000A028
Switch# show authentication sessions detail
Interface   : GigabitEthernet7
MAC Address : 00:01:6C:CB:29:4A
Session ID  : 000000010000A028
Current Type    : dot1x
Status  : Authorized Authorized Information
VLAN    : 5 (from RADIUS)
Reauthenticate Period: 301 (from RADIUS)
Inactive Timeout    : 600 (from RADIUS)
Operational Information VLAN   : 5
Session Time    : 1143
Inactive Time   : 168
Quiet Time  : N/A
```

5. Diagnostic

5.1. show cable-diag

Item	Description
Syntax	show cable-diag interfaces IF_NMLPORTS
Parameter	**interfaces IF_NMLPORTS:** Display the cable diagnostic information of the copper media for an interface ID or a list of interfaces IDs.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	To show the estimated copper cable length attached to a specific interface, use the command show cable-diag in the Privilegeg EXEC mode. For the proper information of the cable length, the interface must be active and linked up.

Example:

The following example shows the result of cable diagnostic for the interface Gi1 and Gi2.

```
Switch# show cable-diag interfaces gi1-2
Port    |   Speed | Local pair | Pair length | Pair status
--------+---------+------------+-------------+---------------
 gi1    |  auto   |  Pair    A | 0.88        |   Open
                    Pair    B | 0.82        |   Open
                    Pair    C | 0.80        |   Open
                    Pair    D | 0.78        |   Open
 gi2    |   auto  | Pair    A | 0.81        |   Open
                    Pair    B | 0.81        |   Open
                    Pair    C | 0.77        |   Open
                    Pair    D | 0.81        |   Open
```

5.2. show fiber-transceiver interfaces

Item	Description
Syntax	show fiber-transceiver interfaces IF_NMLPORTS
Parameter	**interfaces IF_NMLPORTS:** Display the cable diagnostic information of the fiber media for an interface ID or a list of interfaces IDs.
Default	No default value for this command.
Mode	Privileged EXEC

Usage	To show the estimated fiber cable length attached to a specific interface, use the command show fiber-transceiver in the Privilegeg EXEC mode. For the proper information of the cable length, the interface must be active and linked up.

Example:

The following example shows the result of cable diagnostic for the interface Gi1 and Gi2.

```
Switch# show fiber-transceiver interfaces XGigabitEthernet 1-2
Port |Temperature|Voltage|Current| Output power|Input power|OE-Present|LOS
     | [C]       | [Volt]|[mA]   | [mWatt]     | [mWatt]   |          |
================================================================================
xgi1 | N/A       | N/A   | N/A   | N/A         | N/A       | Remove   | Loss
xgi2 | N/A       | N/A   | N/A   | N/A         | N/A       | Remove   | Loss

     Temp        - Internally measured transceiver temperature
     Voltage     - Internally measured supply voltage
     Current     - Measured TX bias current
     Output Power - Measured TX output power in milliWatts
     Input Power  - Measured RX received power in milliWatts
     OE-Present   - SFP Presetn or Not Present
     LOS         - Loss of signal
     N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

5.3. show ip arp inspection

Item	Description
Syntax	show ip arp inspection
	show ip arp inspection interfaces IF_PORTS
	show ip arp inspection interfaces IF_PORTS statistics
Parameter	**interfaces IF_PORTS**: Specify port number
	statistics：Dynamic ARP Inspection Mib counter
Default	No default value for this command.
Mode	User EXEC Privileged EXEC
Usage	Use "**show ip arp inspection**" command to show current ip arp inspection information.

Example:

This example shows how to show current ip arp inspection of the switch.

```
Switch# show ip arp inspection
Dynamic ARP Inspection     : disabled
```

```
    Enable on Vlans           : None
    Switch# show ip arp inspection interfaces GigabitEthernet 24
Interfaces|Trust State|Rate(pps)| SMAC Check|DMAC Check|IP Check/Allow Zero |
----------+-----------+---------+-----------|---------+-------------------+
     gi24 | Untrusted  | None     | disabled  | disabled| disabled/disabled
```

5.4. clear ip arp inspection

Item	Description
Syntax	clear ip arp inspection interfaces IF_PORTS statistics
Parameter	**interfaces IF_PORTS**: Specify port number
	statistics：Dynamic ARP Inspection Mib counter
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show ip arp inspection**" command to clear current ip arp inspection information.

Example:

The example shows how to clear current ip arp inspection information.

```
Switch# clear ip arp inspection interfaces gi1 statistics
```

5.5. ip arp inspection

Item	Description
Syntax	ip arp inspection
	no ip arp inspection
Parameter	
Default	No default value for this command.
Mode	Global Configuration
Usage	Use "**ip arp inspection**" command to enable dynamic ARP inspection state. Use **no** form of this command to disable dynamic arp inspection state.

Example:

This example shows how to setting dynamic ARP Inspection state.

```
Switch(config)# ip arp inspection
Switch(config)# no ip arp inspection
```

5.6. ip arp inspection vlan

Item	Description
Syntax	ip arp inspection vlan VLAN-LIST
	no ip arp inspection vlan VLAN-LIST
Parameter	**VLAN-LIST**: Specifies the VLAN list (e.g. 3,6-8) The range of VLAN ID is 1 to 4094.
Default	No default value for this command.
Mode	Global Configuration
Usage	Use "**ip arp inspection vlan**" command to enabled dynamic ARP inspection VLAN state. Use **no** form of this command to disable dynamic ARP inspection VLAN state.

Example：

This example shows how to setting dynamic ARP Inspection VLAN state.

```
Switch(config)# ip arp inspection vlan 1
```

5.7. ip arp inspection trust

Item	Description
Syntax	ip arp inspection trust
	no ip arp inspection trust
Parameter	
Default	No default value for this command.
Mode	Interface Configuration
Usage	Use "**ip arp inspection trust**" command to setting dynamic ARP inspection port type. Use **no** form of this command to disable dynamic ARP inspection port type.

Example：

This example shows how to setting dynamic ARP inspection Port type.

```
Switch(config-if)# ip arp inspection trust
```

5.8. ip arp inspection validate

Item	Description
Syntax	ip arp inspection validate (src-mac|dst-mac|ip [allow-zeros])

	no ip arp inspection validate (src-mac|dst-mac|ip [allow-zeros])
Parameter	**src-mac**:Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body
	dst-mac:Compare the destination MAC address in the Ethernet header against the target MAC address in the ARP body
	ip:Compare the ARP body for invalid and unexpected IP addresses
	[**allow-zeros**]:Sender address of 0.0.0.0 (ARP probes) are not denied.
Default	No default value for this command.
Mode	Interface Configuration
Usage	Use "**ip arp inspection validate**" command to setting dynamic ARP inspection port check src-mac/dst-mac/ip. Use **no** form of this command to disable dynamic ARP inspection port check src-mac/dst-mac/ip.

Example：

This example shows how to setting dynamic ARP inspection port check src-mac/dst-mac/ip.

```
Switch(config-if)# ip arp inspection validate dst-mac
```

5.9. ip arp inspection rate-limit

Item	Description
Syntax	ip arp inspection rate-limit <1-50>
	no ip arp inspection rate-limit
Parameter	**<1-50>**: Rate limit of arp packets
Default	
Mode	Interface Configuration
Usage	Use "ip arp inspection rate-limit" command to setting ARP limit rate. Use **no** form of this command to disable ARP limit rate.

Example：

This example shows how to setting dynamic ARP limit rate.

```
Switch(config-if)# ip arp inspection rate-limit 20
```

6. DHCP Snooping

6.1. ip dhcp snooping

Item	Description
Syntax	ip dhcp snooping no ip dhcp snooping
Parameter	
Default	DHCP snooping is disabled
Mode	Global Configuration
Usage	Use the i**p dhcp snooping** command to enable DHCP Snooping function. Use the **no** form of this command to disable.

Example:

The example shows how to enable DHCP Snooping on VLAN 1. You can verify settings by the following show ip dhcp snooping command.

```
switch(config)# ip dhcp snooping
switch(config)#ip dhcp snooping vlan 1
switch# show ip dhcp snooping
DHCP Snooping   : enabled
Enable on following Vlans  1
circuit-id default format  : vlan-port
remote-id : 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

6.2. ip dhcp snooping vlan

Item	Description
Syntax	ip dhcp snooping vlan VLAN-LIST
Parameter	**VLAN-LIST:** Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection
Default	Default is disabled on all VLANs
Mode	Global Configuration
Usage	Use the **ip dhcp snooping vlan** command to enable VLANs on DHCP Snooping function. Use the no form of this command to disable VLANs on DHCP Snooping function.

Example:

The example shows how to enable VLAN 1-100 on DHCP Snooping, and then disable

VLAN 30-40 on DHCP Snooping. You can verify settings by the following show ip dhcp snooping command.

```
switch(config)# vlan 1-100 Switch(config-vlan)# exit
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 1-100
switch# show ip dhcp snooping
DHCP Snooping   : enabled
Enable on following Vlans  : 1-100
    circuit-id default format : vlan-port
    remote-id: 00:11:22:33:44:55 (Switch Mac in Byte Order)

switch(config)# no ip dhcp snooping vlan 30-40
switch# show ip dhcp snooping
DHCP Snooping   : enabled
Enable on following Vlans  : 1-29,41-100
    circuit-id default format : vlan-port
    remote-id : 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

6.3. ip dhcp snooping trust

Item	Description
Syntax	ip dhcp snooping trust
	no ip dhcp snooping trust
Parameter	
Default	DHCP snooping trust is disabled
Mode	Interface Configuration
Usage	Use the **ip dhcp snooping trust** command to set trusted interface. The switch does not check DHCP packets that are received on the trusted interface; it simply forwards it. Use the no form of this command to set untrusted interface.

Example:

The example shows how to set interface gi1 to trust. You can verify settings by the following show ip dhcp snooping interface command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping trust
switch(config-if)# do show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
-----------+-------------+-----------+-------------+---------------
```

```
gi1      | Trusted     |   None     |   disabled    | disabled |
```

6.4. ip dhcp snooping verify

Item	Description
Syntax	ip dhcp snooping verify mac-address
	[no] ip dhcp snooping verify mac-address
Parameter	
Default	DHCP snooping verify mac-address is disabled
Mode	Interface Configuration
Usage	Use the **ip dhcp snooping verify** command to verify MAC address function on interface. The "**mac-address**" drop DHCP packets that chaddr and ethernet-source-mac is not match.

Example:

The example shows how to set interface gi1 to validate "mac-address". You can verify settings by the following show ip dhcp snooping interface command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping verify mac-address
switch(config-if)# do show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
-----------+-------------+------------+--------------+-----------------
       gi1 |   Unrusted    |   None    |    disabled   | disabled |
```

6.5. ip dhcp snooping rate-limit

Item	Description
Syntax	ip dhcp snooping rate-limit <1-300>
	[no] ip dhcp snooping rate-limit
Parameter	**<1-300>:** Set 1 to 300 PPS of DHCP packet rate limitation
Default	Default is un-limited of DHCP packet.
Mode	Interface Configuration
Usage	Use the **ip dhcp snooping rate-limit** command to set rate limitation on interface. The switch drop DHCP packets after receives more than configured rate of packets per second. Use the **no** form of this command to return to default settings.

Example:

The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following show ip dhcp snooping interface command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping rate-limit 30
switch(config-if)# do show ip dhcp snooping interfaces gi1
Interfaces|Trust State|Rate (pps)|hwaddr Check|Insert Option82|
----------+-----------+----------+-----------+--------------+
        gi1 | Untrusted |    30     | disabled  | disabled  |
```

6.6. clear ip dhcp snooping statistics

Item	Description
Syntax	clear ip dhcp snooping interfaces IF_PORTS statistics
Parameter	**IF_PORTS**：specifies ports to clear statistics
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **clear ip dhcp snooping interfaces statistics** command to clear statistics that are recorded on interface.

Example:

The example shows how to clear statistics on interface gi1. You can verify settings by the following show ip dhcp snooping interface statistics command.

```
switch# clear ip dhcp snooping interfaces gi1 statistics
switch# show ip dhcp snooping interfaces gi1 statistics
Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust Port With Option82 Dropped | Invalid Drop
----------+----------+--------------------+--------------------+-----------------------------------+-----------
  gi1 |  0   |      0     |     0       |           0          | 0
```

6.7. show ip dhcp snooping

Item	Description
Syntax	show ip dhcp snooping
Parameter	
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show ip dhcp snooping** command to show settings of DHCP Snooping.

Example:

The example shows how to show settings of DHCP Snooping

```
switch# show ip dhcp snooping
DHCP Snooping  : enabled
Enable on following Vlans  : 1
circuit-id default format: vlan-port
remote-id:  : 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

6.8. show ip dhcp snooping interface

Item	Description
Syntax	show ip dhcp snooping interfaces IF_PORTS show ip dhcp snooping interfaces IF_PORTS statistics
Parameter	**IF_PORTS:** specifies ports to show statistics
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show ip dhcp snooping interfaces** command to show settings or statistics of interface.

Example:

The example shows how to show settings of interface gi1.

```
switch# show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
-----------+-------------+------------+--------------+---------------
        gi1 | Untrusted  |     None     |  enabled     | disabled  |
```

The example shows how to show statistics of interface gi1.

```
switch# show ip dhcp snooping interfaces gi1 statistics
Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust Port With Option82 Dropped | Invalid Drop
-----------+-----------+----------------------+----------------------+------------------------------------+-----------
  gi1  | 0   |      0       |     0     |           0         | 0
```

6.9. show ip dhcp snooping binding

Item	Description
Syntax	show ip dhcp snooping binding
Parameter	
Default	No default is defined

Mode	Privileged EXEC
Usage	Use the **show ip dhcp snooping binding** command to show binding entries that learned by DHCP Snooping.

Example:

The example shows how to show binding entries that learned by DHCP Snooping.

```
switch# show ip dhcp snooping binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address   |   IP  |   Type    | Lease Time
-----+------+--------------+-------+-----------+----------
```

6.10. ip dhcp snooping option

Item	Description
Syntax	ip dhcp snooping option
	no ip dhcp snooping option
Parameter	
Default	DHCP snooping option82 is disabled
Mode	Interface Configuration
Usage	Use the **ip dhcp snooping option** command to enable that insert option82 content into packet. Use the **no** form of this command to disable.

Example:

The example shows how to enable option82 insertion. You can verify settings by the following show ip dhcp snooping interface command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping option
switch(config-if)# do show ip dhcp snooping interfaces gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
-----------+-------------+-------------+-------------+-----------------
    gi1    |  Untrusted  |     None    |   disabled   | enabled   |
```

6.11. ip dhcp snooping option action

Item	Description
Syntax	ip dhcp snooping option action (drop|keep|replace)
	no ip dhcp snooping option action
Parameter	**drop:** Drop packets with option82 that are received from un trusted port
	keep: Keep original option82 content in packet

	replace: Replace option82 content by switch setting
Default	DHCP snooping option82 is drop
Mode	Interface Configuration
Usage	Use the **ip dhcp snooping option action** command to set the action when receive packets that with option82 content. Use the **no** form of this command to default setting.

Example:

The example shows how to set action to replace option82 content. You can verify settings by the following show running-config command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping option action replace
```

6.12. ip dhcp snooping option circuit-id

Item	Description
Syntax	ip dhcp snooping [vlan <1-4094>] option circuit-id STRING
	no ip dhcp snooping [vlan <1-4094>] option circuit-id
Parameter	**Vlan <1-4094>:** VLAN ID to set user defined circuit-id string
	STRING: Circuit-id string, 1 to 63 ASCII characters, no spaces.
Default	Default circuit-id is port id + vlan id in byte format.
Mode	Interface Configuration
Usage	Use the **ip dhcp snooping option circuit-id** command to set user-defined circuit-id string. Circuit-id is per port per VLAN setting. If a VLAN is not found user-defined circuit-id then use per port circuit-id string. Use the **no** form of this command to default setting.

Example:

The example shows how to set a user-defined circuit-id string on interface gi1 and VLAN 1. You can verify settings by the following show running-config command

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping vlan 1 option circuit-id test
```

6.13. ip dhcp snooping option remote-id

Item	Description
Syntax	ip dhcp snooping option remote-id STRING
	no ip dhcp snooping option remote-id
Parameter	**STRING:** Remote-id string, 1 to 63 ASCII characters, no spaces.

Default	Default remote-id is the switch MAC address in byte order
Mode	Global Configuration
Usage	Use the **ip dhcp snooping option remote-id** command to set user-defined remote-id string. Remote-id is a global and unique string. Use the **no** form of this command to default setting.

Example:

The example shows how to set a user-defined remote-id string on switch. You can verify settings by the following show ip dhcp snooping option remote- id

```
switch(config)# ip dhcp snooping option remote-id test_remote
switch(config)# do show ip dhcp snooping option remote-id
Remote ID: test_remote
```

6.14. show ip dhcp snooping option

Item	Description
Syntax	show ip dhcp snooping option remote-id
Parameter	
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the s**how ip dhcp snooping option remote-id** command to show remote-id string.

Example:

The example shows how to show remote-id string

```
switch(config)# do show ip dhcp snooping option remote-id
Remote ID: test_remote
```

6.15. ip dhcp snooping database

Item	Description
Syntax	ip dhcp snooping database flash
	ip dhcp snooping database tftp (A.B.C.D|HOSTNAME) NAME
	no ip dhcp snooping database
Parameter	**(A.B.C.D|HOSTNAME):**Specify the IP address or hostname of remote TFTP server.
	NAME: Input name of backup file
Default	DHCP snooping database is disabled

Mode	Global Configuration
Usage	Use the **ip dhcp snooping database** command to enable DHCP Snooping database agent. The "**flash**" means that write backup file to switch local drive. The "**tftp**" means that write backup file to remote TFTP server. Use the **no** form of this command to disable.

Example:

The example shows how to enable DHCP Snooping database agent and write backup file to remote TFTP server with file name "backup_file". You can verify settings by the following show ip dhcp snooping database command.

```
switch(config)# ip dhcp snooping database tftp 192.168.169.56 backup_file
switch(config)# do show ip dhcp snooping database
Type : tftp: 192.168.169.56
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 298

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     1
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

6.16. ip dhcp snooping database write-delay

Item	Description
Syntax	ip dhcp snooping database write-delay <15-86400>
	no ip dhcp snooping database write-delay
Parameter	**<15-86400>:** Specifies the seconds of timeout. Specify the duration for which the transfer should be delayed after the binding database changes
Default	DHCP snooping database write-delay is 300 seconds
Mode	Global Configuration
Usage	Use the **ip dhcp snooping database write-delay** command to modify the write-delay timer. Use the **no** form of this command to default setting.

Example:

The example shows how to set write-delay timer to 60 seconds. You can verify settings by the following show ip dhcp snooping database command.

```
switch(config)# ip dhcp snooping database write-delay 60
switch(config)# do show ip dhcp snooping database
Type : tftp: 192.168.169.56
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 300 seconds

Agent Running : Running
Delay Timer Expiry : 60 seconds
Abort Timer Expiry : 183

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     1
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

6.17. ip dhcp snooping database timeout

Item	Description
Syntax	ip dhcp snooping database timeout <0-86400>
	no ip dhcp snooping database timeout
Parameter	**<15-86400>:** Specifies the seconds of timeout。Specify (in seconds) how long to wait for the database transfer process to finish before stopping the process. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely
Default	DHCP snooping database timeout is 300 seconds
Mode	Global Configuration
Usage	Use the **ip dhcp snooping database timeout** command to modify the timeout timer. Use the **no** form of this command to default setting.

Example:

The example shows how to set timeout timer to 60 seconds. You can verify settings by the following show ip dhcp snooping database command.

```
switch(config)# ip dhcp snooping database timeout 60
switch(config)# do show ip dhcp snooping database

Type : tftp: 192.168.169.56
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 60 seconds

Agent Running : Running
Delay Timer Expiry : 60 seconds
Abort Timer Expiry : 0

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     1
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

6.18. clear ip dhcp snooping database statistics

Item	Description
Syntax	clear ip dhcp snooping database statistics
Parameter	
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **clear ip dhcp snooping database statistics** command to clear statistics of DHCP Snooping databae.

Example:

The example shows how to clear statistics of DHCP Snooping agent. You can verify settings by the following show ip dhcp snooping database command.

```
switch# clear ip dhcp snooping database statistics
switch# show ip dhcp snooping database
Type : tftp: 192.168.169.56
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 60 seconds

Agent Running : None
```

```
Delay Timer Expiry : Not Running
Abort Timer Expiry :Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason :

Total Attempts       :     0
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

6.19. renew ip dhcp snooping database

Item	Description
Syntax	renew ip dhcp snooping database
Parameter	
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show ip dhcp snooping database** command to renew DHCP Snooping database from backup file.

Example:

The example shows how to renew DHCP Snooping database.You can verify settings by the following show ip dhcp snooping database and show ip dhcp snooping binding command.

```
Switch# renew ip dhcp snooping database
switch# show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300
seconds Abort Timer : 60 seconds

Agent Running : Running
Delay Timer Expiry : 300
seconds Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts :   1
Successful Transfers :         1   Failed Transfers :         0
Successful Reads   :   1           Failed Reads:  0
```

```
Successful Writes  :       0       Failed Writes      :       0

switch# show ip dhcp snooping binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address |              IP           |Type| Lease Time
-----+-----+-------------+---------------------------+----------+-----
gi1   | 1 | 48:5B:39:C7:12:62 | 192.168.1.100(255.255.255.255)|DHCP Snooping | 86400
```

6.20. show ip dhcp snooping database

Item	Description
Syntax	show ip dhcp snooping database
Parameter	
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show ip dhcp snooping database** command to show settings of DHCP Snooping agent.

Example:

The example shows how to show settings of DHCP Snooping agent.

```
switch(config)# show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300
seconds Abort Timer : 60 seconds

Agent Running : Running
Delay Timer Expiry : 300
seconds Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts :   1
Successful Transfers : 1       Failed Transfers :         0
Successful Reads   :   1       Failed Reads    :   0
Successful Writes  :       0   Failed Writes      :       0
```

7. DoS

7.1. Dos

Item	Description
Syntax	dos (daeqsa-deny|icmp-frag-pkts-deny|icmpv4-ping-max-check|icmpv6-ping-max-check|ipv6-min-frag-size-check|land-deny|nullscan-deny|pod-deny|smurf-deny|syn-sportl1024-deny|synfin-deny|synrst-deny|tcp-frag-off-min-check|tcpblat-deny|tcphdr-min-check|udpblat-deny|xmas-deny)
	dos icmp-ping-max-length MAX_LEN
	dos ipv6-min-frag-size-length MIN_LEN
	dos smurf-netmask MASK
	dos tcphdr-min-length HDR_MIN_LEN
	no dos (tcp-frag-off-min-check|synrst-deny|synfin-deny|xma-deny|nullscan-deny|syn-sportl1024-deny|tcphdr-min-check|smurf-deny|icmpv6-ping-max-check|icmpv4-ping-max-check|icmp-frag-pkts-deny|ipv6-min-frag-size-check|pod-deny|tcpblat-deny|udpblat-deny|land-deny|daeqsa-deny)
Parameter	**daeqsa-deny:** Drops the packets if the destination MAC address is equal to the source MAC address.
	icmp-frag-pkts- deny:Drops the fragmented ICMP packets.
	icmpv4-ping-max- check:Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size defined by the command dos icmp-ping-max-length MAX_LEN.
	icmpv6-ping-max- check: Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size defined by the command dos icmp-ping-max- length MAX_LEN.
	ipv6-min-frag- size-check:Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size defined by the command dos ipv6-min-frag-size-length MIN_LEN.
	land-deny: Drops the packets if the source IP address is equal to the destination IP address.
	nullscan-deny: Drops the packets with NULL scan.
	pod-deny: Avoids ping of death attack.
	smurf-deny: Avoids smurf attack.
	syn-sportl1024- deny: Drops SYN packets with sport less than 1024.
	synfin-deny: Drops the packets with SYN and FIN bits set.
	synrst-deny: Drops the packets with SYN and RST bits set.
	tcp-frag-off-min- check:Drops the TCP fragment packets with offset equals to one.
	tcpblat-deny: Drops the packages if the TCP source port is equal to the TCP destination port.

	tcphdr-min-check: Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size defined by the command dos tcphdr-min-length HDR_MIN_LEN.
	udpblat-deny: Drops the packets if the UDP source port equals to the UDP destination port.
	xmas-deny: Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
	icmp-ping-max- length MAX_LEN: Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
	ipv6-min-frag- size-length MIN_LEN: Specify the minimum size of IPv6 fragments. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.
	smurf-netmask MASK: Specify the netmask of smurf attack. The length range is from 0 to 323 bytes, and default length is 0 bytes.
	tcphdr-min-length HDR_MIN_LEN: Specify the minimum TCP header length. The length range is from 0 to 31 bytes, and default length is 20bytes.
Default	All of DoS protections are enabled by default. The default parameter are: The maximum size of ICMP ping packages is 512 bytes The minimum size of IPv6 fragments is 1240 bytes. The Smurf netmask length is 0 bytes. The minimum TCP header length is 20 bytes.
Mode	Global Configuration
Usage	To enable the specific Deniel of Service (DoS) protection, use the command **dos** in the Global Configuration mode. Otherwise, use the **no** form of the command to disable the specific DoS protection.

Example:

The following example sets the minimum fragment size to 1024 bytes, and enables the minimum size of IPv6 fragments validation.

```
Switch(config)# dos ipv6-min-frag-size-length 1024
Switch(config)# dos ipv6-min-frag-size-check
```

7.2. dos (interface)

Item	Description
Syntax	dos
	no dos
Parameter	
Default	DoS protection is disabled on each interface.

Mode	Interface Configuration
Usage	To enable the **DoS** on the specific interface, use the command dos in the Interface Configuration mode. Otherwise, use the **no** form of the command to disable the DoS on the interface.

Example:

The following example enables the DoS on the interface GigabitEthernet1.

```
Switch(config)# interface Gi1
Switch(config-if)# dos
```

7.3. show dos

Item	Description
Syntax	show dos
	show dos interface IF_PORTS
Parameter	**interface IF_PORT**S: An interface ID or the list of interface IDs.
Default	DoS protection is disabled on each interface.
Mode	Privileged EXEC
Usage	To show the DoS protection configuration, use the command **show dos** in the Privileged EXEC mode. For the status of DoS protection on each interface, use the command **show dos interface** in the Priveleged EXEC mode.

Example:

The following example shows the global DoS protection configuration.

```
Switch# show dos
Type                     | State (Length)
-------------------------+--------------------------------
DMAC equal to SMAC       | enabled
Land (DIP = SIP)         | enabled
UDP Blat (DPORT = SPORT) | enabled
TCP Blat (DPORT = SPORT) | enabled
POD (Ping of Death)      | enabled
IPv6 Min Fragment Size   | enabled  (1024 Bytes)
ICMP Fragment Packets    | enabled
IPv4 Ping Max Packet Size |        enabled   (512 Bytes)
IPv6 Ping Max Packet Size |        enabled   (512 Bytes)
Smurf Attack             | enabled  (Netmask Length: 0)
TCP Min Header Length    | enabled  (20 Bytes)
TCP Syn (SPORT < 1024)   | enabled
Null Scan Attack         | enabled
X-Mas Scan Attack        | enabled
```

```
TCP SYN-FIN Attack       | enabled
TCP SYN-RST Attack       | enabled
TCP Fragment (Offset = 1)  |        enabled
```

The following example shows the status of DoS protection on the interface GigabitEthernet1.

```
Switch# show dos interfaces GigabitEthernet1
Port      | DoS Protection
----------+---------------
     gi1  | disabled
```

8. IGMP Snooping

8.1. ip igmp snooping

Item	Description
Syntax	ip igmp snooping no ip igmp snooping
Parameter	
Default	Default is enabled
Mode	Global Configuration
Usage	Use the **ip igmp snooping** command to enable IGMP snooping function. Use the **no** form of this command to disable. You can verify settings by the **show ip igmp snooping** command.

Example:

The following example specifies that set ip igmp snooping test.

```
Switch(config)# no ip igmp snooping
Switch(config)#show ip igmp snooping
               IGMP Snooping Status
               --------------------
    Snooping                      : Enabled
    Report Suppression            : Enabled
    Operation Version             : v2
    Forward Method                : mac
    Unknown IP Multicast Action   : Flood

               Packet Statistics
    Total RX                      :  4330
    Valid RX                      :  1
    Invalid RX                    :  4329
    Other RX                      :  0
    Leave RX                      :  0
    Report RX                     :  0
    General Query RX              :  0
    Specail Group Query RX        :  0
    Specail Group & Source Query RX  :  0
    Leave TX                      :  0
    Report TX                     :  0
    General Query TX              :  0
    Specail Group Query TX        :  0
    Specail Group & Source Query TX  :  0
```

8.2. ip igmp snooping report-suppression

Item	Description
Syntax	ip igmp snooping report-suppression no ip igmp snooping report-suppression
Parameter	
Default	Default is enabled
Mode	Global Configuration
Usage	Use the **ip igmp snooping report-suppression** command to enable IGMP snooping report-suppression function. Use the **no** form of this command to disable. Disable report-supression will forward all received reports to the vlan router ports. You can verify settings by the show ip igmp snooping command.

Example:

The following example specifies that disable ip igmp snooping report-suppression test.

```
Switch(config)# ip igmp snooping report-suppression
Switch# show ip igmp snooping
                IGMP Snooping Status
                --------------------

    Snooping                      : Enabled
    Report Suppression             : Enabled
    Operation Version              : v2
    Forward Method                 : mac
    Unknown IP Multicast Action     : Flood
.....................................
```

8.3. ip igmp snooping version

Item	Description
Syntax	ip igmp snooping version (2|3)
Parameter	**(2|3):** IGMP version 2 or IGMP version 3 basic mode
Default	Default is version 2
Mode	Global Configuration
Usage	Use the **ip igmp snooping version** command to change IGMP support version. Only basic mode is supported in v3. When change version from v3 to v2, all querier version will update to version 2. You can verify settings by the **show ip igmp snooping** command.

Example:

The following example specifies that set ip igmp snooping version 3.

```
Switch(config)# ip igmp snooping version 3
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------
Snooping                        : Disabled
Report Suppression              : Enabled
Operation Version               : v3
Forward Method                  : mac
Unknown IP Multicast Action     : Flood
.................
```

8.4. ip igmp snooping unknown-multicast action

Item	Description
Syntax	ip igmp snooping unknown-multicast action (drop | flood |router-port) no ip igmp snooping unknown-multicast action
Parameter	**(drop | flood | router- port):** Drop、flood in vlan or forward to router port of unknown multicast packet
Default	Default is flood.
Mode	Global Configuration
Usage	When igmp and mld snooping disabled, it can't set action router-port. When disable igmp snooping & mld snooping, it set unknown multicast action flood. When action is router-port to flood or drop, it will delete the unknown multicast group entry. Use the **ip igmp snooping unknown-multicast action** command to change action. Use the **no** form of this command to restore to default. You can verify settings by the show ip igmp snooping command.

Example:

The following example specifies that set ip igmp unknown multicast action router-port test.

```
Switch(config)# ip igmp snooping
Switch(config)# ip igmp snooping unknown-multicast action router-port
Switch# show ip igmp snooping
 IGMP Snooping Status
                --------------------
   Snooping                        : Enabled
```

```
Report Suppression              : Enabled
Operation Version               : v3
Forward Method                  : mac
Unknown IP Multicast Action     : Router-Port
           Packet Statistics
Total RX                        :  0
Valid RX                        :  0
Invalid RX                      :  0
Other RX                        :  0
Leave RX                        :  0
Report RX                       :  0
General Query RX                :  0
Specail Group Query RX          :  0
Specail Group & Source Query RX  :  0
Leave TX                        :  0
Report TX                       :  0
General Query TX                :  0
Specail Group Query TX          :  0
Specail Group & Source Query TX  :  0
```

8.5. ip igmp snooping querier

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> querier [version (2|3)]
	no ip igmp snooping [vlan <VLAN-LIST>] querier
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	(2|3): Query version 2 or 3
Default	No ip igmp snooping querier by default
Mode	Global Configuration
Usage	When enable ip igmp vlan querier, there will process router select, the select successful will send general and specific query. Use the **ip igmp snooping querier** command to add querier. Use the **no** form of this command to delete querier. You can verify settings by the show **ip igmp snooping querier** command.

Example:

The following example specifies that set ip igmp snooping querier test.

```
Switch(config)# ip igmp snooping vlan 2 querier version 3
Switch# show ip igmp snooping querier
  VID  |    State    |    Status   | Version   |  Querier IP
-------+-------------+-------------+-----------+--------------------
    1  |  Disabled   | Non-Querier |   No      |    ------
```

```
Total Entry 1
```

8.6. ip igmp snooping vlan

Item	Description
Syntax	ip igmp snooping vlan VLAN-LIST
	no ip igmp snooping vlan VLAN-LIST
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
Default	Default is disabled for all VLANs
Mode	Global Configuration
Usage	Disable will clear all ip igmp snooping dynamic group and dynamic router port and make all static ip igmp group invalid of this vlan. Will not learn dynamic group and router port by igmp message any more. Use the **ip igmp snooping vlan** command to enable IGMP on VLAN. Use the **no** form of this command to disable You can verify settings by the **show ip igmp snooping vlan** command.

Example:

The following example specifies that set ip igmp snooping vlan test.

```
Switch(config)# ip igmp snooping
Switch(config)# ip igmp snooping vlan 2
```

8.7. ip igmp snooping vlan fastleave

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> fastleave
	no ip igmp snooping vlan <VLAN-LIST> fastleave
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
Default	Default is disabled
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan fastleave** command to enable fastleave function. Group will remove port immediately when receive leave packet. Use the **no** form of this command to disable. You can verify settings by the **show ip igmp snooping vlan** command

Example：

The following example specifies that set ip igmp snooping vlan fastleave test.

```
Switch(config)# ip igmp snooping vlan 1 fastleave
```

8.8. ip igmp snooping vlan last-member-query-count

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> last-member-query-count <1-7>
	no ip igmp snooping vlan <VLAN-LIST> last-member-query-count
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	last-member-query-count <1-7>:specifies last member query count to set.
Default	Default is 2
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan last-member-query-count** command to change how many query packets will send. Use the **no** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command

Example:

The following example specifies that set ip igmp snooping vlan last-member-query-count test.

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-count 5
```

8.9. ip igmp snooping vlan last-member-query-interval

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> last-member-query-interval <1- 7>
	no ip igmp snooping vlan <VLAN-LIST> last-member-query-interval
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	last-member-query-interval <1-7>：specifies last member query interval to set
Default	Default is 1
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan last-member-query-interval** command to set interval between each query packet. Use the **no** form of this command to restore to default You can verify settings by the **show ip igmp snooping vlan** command

Example:

The following example specifies that set ip igmp snooping vlan last-member-query-interval test.

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3
```

8.10. ip igmp snooping vlan query-interval

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> query-interval <30-18000>
	no ip igmp snooping vlan <VLAN-LIST> query-interval
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	query-interval <30-18000>: specifies query interval to set
Default	Default is 125
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan query-interval** command to set interval between each query. Use the **no** form of this command to restore to default You can verify settings by the **show ip igmp snooping vlan** command

Example:

The following example specifies that set ip igmp snooping vlan query-interval test.

```
Switch(config)# ip igmp snooping vlan 1 query-interval 100
```

8.11. ip igmp snooping vlan response-time

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> response-time <5-20>
	no ip igmp snooping vlan <VLAN-LIST> response-time
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	response-time <5-20>: specifies a response time to set
Default	Default is 10
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan response-time** command to set response time Use the **no** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command

Example:

The following example specifies that set ip igmp snooping vlan response-time test.

```
Switch(config)# ip igmp snooping vlan 1 response-time 12
```

8.12. ip igmp snooping vlan robustness-variable

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> robustness-variable <1-7>
	no ip igmp snooping vlan <VLAN-LIST> robustness-variable
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	robustness-variable<1-7>： specifies a robustness value to set
Default	Default is 2
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan robustness-variable** command to times to retry. Use the **no** form of this command to restore to default You can verify settings by the **show ip igmp snooping vlan** command

Example:

The following example specifies that set ip igmp snooping vlan parameters test.

```
Switch(config)# ip igmp snooping vlan 1 robustness-variable 1
```

8.13. ip igmp snooping vlan router

Item	Description
Syntax	ip igmp snooping vlan VLAN-LIST router learn pim-dvmrp
	no ip igmp snooping vlan VLAN-LIST router learn pim-dvmrp
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
Default	Default is enabled
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan router** command to enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the **no** form of this command to disable. You can verify settings by the **show ip igmp snooping vlan** command

Example:

The following example specifies that set ip igmp snooping vlan router learn pim-dvmrp test.

```
Switch(config)# ip igmp snooping vlan 99 router learn pim-dvmrp
```

8.14. ip igmp snooping vlan forbidden-port

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> forbidden-port IF_PORTS
	no ip igmp snooping vlan <VLAN-LIST> forbidden-port IF_PORTS
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	IF_PORTS: specifies a port list to set or remove
Default	No forbidden ports by default
Mode	Global Configuration
Usage	'ip igmp snooping vlan 1 static-port gi1-2' will add static port gi1-2 for vlan the all known vlan 1 ipv4 group will add the static ports. 'ip igmp snooping vlan 1 forbidden-port gi3-4' will add forbidden port gi3-4 for vlan 1.the all known vlan 1 ipv4 group will remove the forbidden ports. The configure can use 'show ip igmp snooping forward-all'. Use the **ip igmp snooping vlan forbidden-port** command to add static non- forwarding port, all known vlan 1 ipv4 group will remove the forbidden ports. Use the **no** form of this command to delete forbidden port. You can verify settings by the **show ip igmp snooping forward-all** command

Example:

The following example specifies that set ip igmp snooping static/forbidden port test.

```
Switch(config)# ip igmp snooping vlan 1 forbidden-port gi3-4
```

8.15. ip igmp snooping vlan static-port

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> static-port IF_PORTS
	no ip igmp snooping vlan <VLAN-LIST> static-port IF_PORTS
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	IF_PORTS: specifies a port list to set or remove
Default	No static port by default
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan static-port** command to add static forwarding port, all known vlan 1 ipv4 group will add the static ports. Use the **no** form of this command to delete static port. You can verify settings by the **show ip igmp snooping forward-all** command.

Example:

The following example specifies that set ip igmp snooping static port test.

```
Switch(config)# ip igmp snooping vlan 1 static-port gi1-2
```

8.16. ip igmp snooping vlan forbidden-router-port

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS
	no ip igmp snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	IF_PORTS: specifies a port list to set or remove
Default	No forbidden router ports by default
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan forbidden-router-port** command to add static forbidden router port. This will also remove port from static router port. The forbidden router port will not forward received query packet .Use the **no** form of this command to delete forbidden router port. You can verify settings by the **show ip igmp snooping router** command.

Example:

The following example specifies that set ip igmp snooping forbidden test.

```
Switch(config)# ip igmp snooping vlan 1 forbidden-router-port gi2
```

8.17. ip igmp snooping vlan static-router-port

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> static-router-port IF_PORTS
	no ip igmp snooping vlan <VLAN-LIST> static-router-port IF_PORTS
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	IF_PORTS: specifies a port list to set or remove
Default	No static router ports by default
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan static-router-port** command to add static router port. All query packets will forward to this port. Use the **no** form of this command to delete static router port. You can verify settings by the **show ip igmp snooping router** command.

Example:

The following example specifies that set ip igmp snooping static test.

```
Switch(config)# ip igmp snooping vlan 1 static-router-port gi1-2
```

8.18. ip igmp snooping vlan static-group

Item	Description
Syntax	ip igmp snooping vlan <VLAN-LIST> static-group [<ip-addr>] interfaces IF_PORTS
	no ip igmp snooping vlan <VLAN-LIST> static-group <ip-addr> interfaces IF_PORTS
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	ip-addr: specifies multicast group ipv4 address
	IF_PORTS: specifies a port list to set or remove
Default	No static group by default
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan static-group** command to add a static group.The static group will not learn other dynamic ports. If the dynamic group exists, then the static group will overlap the dynamic group. The static group set to valid unless igmp snooping global and vlan enable. Use the **no** form of this command to delete a port in static group. If remove the last member of static group, the static group will be delete. You can verify settings by the **show ip igmp snooping group** command.

Example:

The following example specifies that set ip igmp snooping static group test.

```
Switch(config)# ip igmp snooping vlan 1 static-group 224.1.1.1 interfaces gi1-2
```

8.19. ip igmp snooping vlan group

Item	Description
Syntax	no ip igmp snooping vlan <VLAN-LIST> group <ip-addr>
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
	ip-addr: specifies multicast group ipv4 address
Default	None
Mode	Global Configuration
Usage	Use the **no ip igmp snooping vlan group** command to delete a group which could be static or dynamic. You can verify settings by the **show ip igmp snooping group** command.

Example:

The following example specifies that set ip igmp snooping static group test.

```
Switch(config)# no ip igmp snooping vlan 1 group 224.1.1.1
```

8.20. ip igmp snooping vlan immediate-leave

Item	Description
Syntax	ip igmp snooping vlan VLAN-LIST immediate-leave
	no ip igmp snooping vlan VLAN-LIST immediate-leave
Parameter	**VLAN-LIST:** specifies VLAN ID list to set
Default	
Mode	Global Configuration
Usage	Use the **ip igmp snooping vlan immediate-leave** command to enable immediate-leave function. Use the **no** form of this command to disable.

Example：

The following example specifies that set ip igmp snooping vlan immediate-leave test.

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

8.21. ip igmp snooping forward-method

Item	Description
Syntax	ip igmp snooping forward-method (mac|dip)
Parameter	**mac:** Specify the MAC method
	dip:Specify the DIP method
Default	Default is mac mode
Mode	Global Configuration
Usage	Use the **ip igmp snooping forward-method** command to igmp lookup mode.

Example：

The following example specifies that setip igmp snooping forward-method test.

```
Switch(config)# ip igmp snooping forward-method dip
```

8.22. profile range

Item	Description
Syntax	profile range ip <ip-addr> [ip-addr] action (permit | deny)
Parameter	**<ip-addr>**：Start ipv4 multicast address
	[ip-addr]: End ipv4 multicast address
	(permit | deny): Permit: allow Multicast address range ip address Learning deny: do not allow Multicast address range ip address learning
Default	None
Mode	igmp profile configuration mode
Usage	Use the **profile** command to generate IGMP profile. You can verify settings by the **show ip igmp profile** command

Example:

The following example specifies that set ip igmp profile test.

```
Switch(config)# ip igmp profile 1
Switch(config-igmp-profile)# profile range ip 224.1.1.1 224.1.1.8 action permit
```

8.23. ip igmp profile

Item	Description
Syntax	ip igmp profile <1-128>
	no ip igmp profile <1-128>
Parameter	**<1-128>:** specifies profile ID
Default	No profie exist by default
Mode	Global Configuration
Usage	Use the **ip igmp profile** command to enter profile configuration Use the **no** form of this command to delete profile You can verify settings by the **show ip igmp profile** command

Example：

The following example specifies that set ip igmp profile test.

```
Switch(config)# ip igmp profile 1
```

8.24. ip igmp filter

Item	Description
Syntax	ip igmp filter <1-128>
	[no] ip igmp filter
Parameter	**<1-128>:** specifies profile ID
Default	
Mode	Port Configuration
Usage	Use the **ip igmp filter** command to bind a profile for port. When the port bind a profile. Then the port learning group will update, if the group is not match the profile rule it will remove the port from the group. Static group is excluded. Use the **no** form of this command to delete profile You can verify settings by the **show ip igmp filter** command

Example:

The following example specifies that set ip igmp filter test.

```
Switch(config)# interface gi1
Switch(config-if)#ip igmp filter 1
```

8.25. ip igmp max-groups

Item	Description
Syntax	ip igmp max-groups <0-1024>
	no ip igmp max-groups
Parameter	**<0-1024>:** The maximum number of IGMP groups that an interface can join.
Default	Default is 1024
Mode	Port Configuration
Usage	Use the **ip igmp max-groups** command to limit port learning max group number. When the port has reach limitation, new group will not add this port. Static group is excluded. Use the **no** form of this command to restore to default You can verify settings by the **show ip igmp max-group** command.

Example:

The following example specifies that set ip igmp max-groups test.

```
Switch(config-if)#ip igmp max-groups 10
```

8.26. ip igmp max-groups action

Item	Description
Syntax	ip igmp max-groups action (deny | replace)
Parameter	**(deny | replace):** Deny: current port igmp group arrived max-groups, don't add group.Replace: current port igmp group arrived max-groups, remove port for rand group, and add port to new group.
Default	Default action is deny
Mode	Port Configuration
Usage	Use the **ip igmp max-groups action** command to set the action when the numbers of groups reach the limitation. Use the **no** form of this command to restore to default You can verify settings by the **show ip igmp max-group** command.

Example:

The following example specifies that set action replace test.

```
Switch(config-if)#ip igmp max-groups action replace
```

8.27. clear ip igmp snooping groups

Item	Description
Syntax	clear ip igmp snooping groups [(dynamic | static)]
Parameter	none Clear ip igmp groups include dynamic and static
	(dynamic | static): Ip igmp group type is dynamic or static
Default	
Mode	Privileged EXEC
Usage	This command will clear the ip igmp groups for dynamic or static or all of type. You can verify settings by the **show ip igmp snooping groups** command.

Example:

The following example specifies that clear ip igmp snooping groups test.

```
Switch# clear ip igmp snooping groups
Switch# show ip igmp snooping groups
VLAN | Group IP Address | Type | Life(Sec) | Port
------+-----------------+--------+-----------+-----------------
```

```
Total Number of Entry = 0
```

8.28. clear ip igmp snooping statistics

Item	Description
Syntax	clear ip igmp snooping statistics
Parameter	
Default	
Mode	Privileged EXEC
Usage	This command will clear the igmp statistics. You can verify settings by the **show ip igmp snooping** command.

Example:

The following example specifies that clear ip igmp snooping statistics test.

```
Switch# clear ip igmp snooping statistics
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------

Snooping    : Enabled
Report Suppression     : Enabled
Operation Version  : v2
Forward Method  : mac
Unknown IP Multicast Action    : Flood

Packet Statistics
Total RX    :  0
Valid RX    :  0
Invalid RX  : 0
Other RX    : 0
Leave RX    : 0
Report RX   :  0
General Query RX       : 0 S
pecail Group Query RX          : 0
Specail Group & Source Query RX : 0
Leave TX    : 0
Report TX   :  0
General Query TX    : 0
Specail Group Query TX     : 0
Specail Group & Source Query TX : 0
```

8.29. show ip igmp snooping groups counters

Item	Description
Syntax	show ip igmp snooping groups counters
Parameter	
Default	
Mode	Privileged EXEC
Usage	This command will display the **ip igmp group counter** include static group.

Example:

The following example specifies that display ip igmp snooping group counter test.

Switch# **show ip igmp snooping groups counters**

Total ip igmp snooping group number: 2

Total ip igmp snooping static mac number: 0

8.30. show ip igmp snooping groups

Item	Description
Syntax	show ip igmp snooping groups [(dynamic | static)]
Parameter	none Show ip igmp groups include dynamic and static
	(dynamic | static): Display Ip igmp group type is dynamic or static
Default	
Mode	Privileged EXEC
Usage	This command will display the ip igmp groups for dynamic or static or all of type.

Example:

The following example specifies that show ip igmp snooping groups.

```
Switch# show ip igmp snooping groups
VLAN | Group IP Address | Type | Life(Sec) | Port
------+-----------------+-------+----------+------------------
    1 |     224.1.2.3    | Static|  --      | fa9
    1 |     224.1.2.4    | Static|  --      | gi10

  Total Number of Entry = 2
```

8.31. show ip igmp snooping router

Item	Description
Syntax	show ip igmp snooping router [(dynamic | forbidden |static)]
Parameter	none Show ip igmp router include dynamic and static and forbidden
	(dynamic |forbidden | static): Display Ip igmp router info for different type
Default	
Mode	Privileged EXEC
Usage	This command will display the ip igmp router info.

Example:

The following example specifies that show ip igmp snooping router.

```
Switch# show ip igmp snooping router
Dynamic Router Table
 VID  |  Port   | Expiry Time(Sec)
------+---------+-----------------

Total Entry 0

Static Router Table
VID  | Port Mask
------+-----------------------
   1 | gi1-2


Total Entry 1


Forbidden Router Table
 VID  | Port Mask
------+-----------------------

Total Entry 0
```

8.32. show ip igmp snooping querier

Item	Description
Syntax	show ip igmp snooping querier
Parameter	none Show all vlan ip igmp querier info.

Default	
Mode	Privileged EXEC
Usage	This command will display all of the static vlan ip igmp querier info.

Example:

The following example specifies that show ip igmp snooping querier test.

```
Switch# show ip igmp snooping querier
VID |   State   |   Status | Version | Querier IP
----+-----------+---------+---------+-------------------
 1 |  Disabled   | Non-Querier |  No   |   ------

  Total Entry 1
```

8.33. show ip igmp snooping

Item	Description
Syntax	show ip igmp snooping
Parameter	
Default	
Mode	Privileged EXEC
Usage	This command will display ip igmp snooping global info.

Example:

The following example specifies that show ip igmp snooping test.

```
Switch# show ip igmp snooping
            IGMP Snooping Status
            --------------------

Snooping    : Enabled
Report Suppression     : Enabled
Operation Version   : v2
Forward Method  : mac
Unknown Multicast Action       : Flood
        Packet Statistics
Total RX    :  0
Valid RX    :  0
Invalid RX  : 0
Other RX    : 0
Leave RX    :  0
Report RX   :  0
```

```
General Query RX       : 0
Specail Group Query RX         : 0
Specail Group & Source Query RX : 0
Leave TX    : 0
Report TX   : 0
General Query TX    : 0
Specail Group Query TX     : 0
Specail Group & Source Query TX : 0
```

8.34. show ip igmp snooping vlan

Item	Description
Syntax	show ip igmp snooping vlan [VLAN-LIST]
Parameter	none Show all ip igmp snooping vlan info
	[VLAN-LIST]: Show specifies vlan ip igmp snooping info
Default	
Mode	Privileged EXEC
Usage	This command will display ip igmp snooping vlan info.

Example:

The following example specifies that show ip igmp snooping vlan test.

```
Switch# show ip igmp snooping vlan 1
IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 1 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 12 sec oper 10 sec
IGMP Snooping last member query counter: admin 5 oper 2
IGMP Snooping last member query interval: admin 3 sec oper 1 sec
IGMP Snooping last immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

8.35. show ip igmp snooping forward-all

Item	Description
Syntax	show ip igmp snooping forward-all [vlan VLAN-LIST]
Parameter	none Show all ip igmp snooping vlan forward-all info
	[vlan VLAN-LIST]: Show specifies vlan of ip igmp forward info.

Default	
Mode	Privileged EXEC
Usage	This command will display ip igmp snooping forward all info.

Example:

The following example specifies that show ip igmp snooping forward-all test.

```
Switch# show ip igmp snooping forward-all vlan 1
IGMP Snooping VLAN 1
IGMP Snooping static port  : None
IGMP Snooping forbidden port : None
```

8.36. show ip igmp profile

Item	Description
Syntax	show ip igmp profile [<1-128>]
Parameter	none Show all ip igmp snooping profile info
	[<1-128>] Show specifies index profile info
Default	
Mode	Privileged EXEC
Usage	This command will display ip igmp profile info.

Example:

The following example specifies that show ip igmp profile test.

```
Switch# show ip igmp profile
IP igmp profile index: 1
IP igmp profile action: permit
Range low ip: 224.1.1.1
Range high ip: 224.1.1.8

IP igmp profile index: 2
IP igmp profile action: deny
Range low ip: 225.1.1.0
Range high ip: 225.1.2.1
```

8.37. show ip igmp filter

Item	Description
Syntax	show ip igmp filter [interfaces IF_PORTS]

Parameter	none Show all port filter
	[interfaces IF_PORTS]: Show specifies ports filter
Default	
Mode	Privileged EXEC
Usage	This command will display ip igmp port filter info.

Example:

The following example specifies that show ip igmp filter test.

```
Switch# show ip igmp filter
Port ID  |  Profile ID
---------+--------------
gi1 : 1
gi2 : None gi3 : None gi4 : None gi5 : None
  --More--
```

8.38. show ip igmp max-group

Item	Description
Syntax	show ip igmp max-group [interfaces IF_PORTS]
Parameter	none Show all port max-group
	[interfaces IF_PORTS]: Show specifies ports max-group
Default	
Mode	Privileged EXEC
Usage	This command will display ip igmp port max-group.

Example:

The following example specifies that show ip igmp max-group test.

```
Switch(config)# interface gi1
Switch(config-if)#ip igmp max-groups 50
Switch# show ip igmp max-group
Port ID | Max Group
--------+--------------
    gi1 : 50
    gi2 : 256
    gi3 : 256
    gi4 : 256
    gi5 : 256
          --More--
```

8.39. show ip igmp max-group action

Item	Description
Syntax	show ip igmp max-group action [interfaces IF_PORTS]
Parameter	none Show all port max-group action
	[interfaces IF_PORTS]: Show specifies ports max-group action
Default	
Mode	Privileged EXEC
Usage	This command will display ip igmp port max-group action.

Example:

The following example specifies that show ip igmp max-group action test.

```
Switch(config)#interface gi1
Switch(config-if)#ip igmp max-groups action replace
Switch# show ip igmp max-group action
Port ID | Max-groups Action
--------+--------------------
    gi1 : replace
    gi2 : deny
    gi3 : deny
    gi4 : deny
    gi5 : deny
          --More—
```

9. IP Source Guard

9.1. ip source verify

Item	Description
Syntax	ip source verify [mac-and-ip]
	no ip source verify
Parameter	**mac-and-ip:** Verify by mac and ip address boundle
Default	IP Source Guard is disabled on interface. Default is that verifying ip address only
Mode	Port Configuration
Usage	Use the **ip source verify** command to enable IP Source Guard function. Default IP Source Guard filter source IP address. The "mac-and-ip" filters not only source IP address but also source MAC address. Use the **no** form of this command to disable. You can verify settings by the **show ip source interfaces** command.

Example:

The example shows how to enable IP Source Guard with source IP address filtering on interface gi1.

```
Switch(config)# interface gi1
switch(config-if)# ip source verify
```

The example shows how to enable IP Source Guard with source IP and MAC address filtering on interface gi2.

```
Switch(config)# interface gi2
switch(config-if)# ip source verify mac-and-ip
switch(config-if)# do show ip source interfaces gi1-2
Port  | Status  | Max Entry | Current Entry
------+--------+-----------+--------------
gi1 | Verify MAC+IP | No Limit | 0
gi2 |   disabled | No Limit | 0
```

9.2. ip source binding

Item	Description
Syntax	ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT
	no ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT

	ip source binding vlan <1-4094> A.B.C.D A.B.C.D interface IF_PORT
	no ip source binding vlan <1-4094> A.B.C.D A.B.C.D interface IF_PORT
	ip source binding max-entry (<1-50>|no-limit)
Parameter	**A:B:C:D:E:F**:Specify a MAC address of a binding entry
	VLAN <1-4094>: Specify a VLAN ID of a binding entry
	A.B.C.D: Specify IP address and MASK of a binding entry.
	IF_PORT: Specify interface of a binding entry.
Default	Default is no binding entry.
Mode	Global Configuration
Usage	Use the **ip source binding** command to create a static IP source binding entry has an IP address, its associated MAC address、VLAN ID、interface. Use the **no** form of this command to delete static entry. You can verify settings by the **show ip source binding** command.

Example:

The example shows how to add a static IP source binding entry.

```
Switch(config)# ip source binding 00:11:22:33:44:55 vlan 1 192.168.1.55
interface GigabitEthernet1
switch(config)# do show ip source binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address  |    IP  | Type | Lease Time
----+---+-------------------+-------------+-----------+-----------
 gi1| 1 | 00:11:22:33:44:55 |192.168.1.55(255.255.255.255)| Static | NA
```

9.3. show ip source interface

Item	Description
Syntax	show ip source interfaces IF_PORTS
	no ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT
	ip source binding vlan <1-4094> A.B.C.D A.B.C.D interface IF_PORT
	no ip source binding vlan <1-4094> A.B.C.D A.B.C.D interface IF_PORT
	ip source binding max-entry (<1-50>|no-limit)
Parameter	**IF_PORTS:** specifies ports to show
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show ip source interface** command to show settings of IP Source Guard of interface

Example:

The example shows how to show settings of IP Source Guard of interface gi1

```
switch# show ip source interfaces gi1
```

```
Port  |     Status      | Max Entry | Current Entry
------+-----------------+-----------+---------------
  gi1 |  Verify MAC+IP  |  No Limit  | 0
```

9.4. show ip source binding

Item	Description
Syntax	show ip source binding [(dynamic|static)]
Parameter	**dynamic:** Show entries that added by DHCP snooping learn
	static: Show entries that added by user
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show ip source binding** command to show binding entries of IP Source Guard.

Example:

The example shows how to show static binding entries of IP Source Guard.

```
switch# show ip source binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address  |           IP              | Type | Lease Time
----+------+-------------+---------------------------+------------+----
gi1 | 1 | 00:11:22:33:44:55 |192.168.1.55(255.255.255.255)| Static | NA
```

10. Link Aggregation

10.1. Lag

Item	Description
Syntax	lag <1-8> mode (static | active | passive)
	no lag
Parameter	**<1-8>:** Specify the LAG id for the interface
	static: Specify the LAG to be static mode and join the interface into this LAG.
	active: Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port.
	passive: Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port.
Default	There is no LAG in default.
Mode	Interface Configuration
Usage	Link aggregation group function allows you to aggregate multiple physical ports into one logic port to increase bandwidth. This command makes normal port join into the specific LAG logic port with static or dynamic mode. And use "**no lag**" to leave the LAG logic port.

Example:

This example shows how to create a dynamic LAG and join gi1-fa3 to thisLAG.

```
Switch(config)# interface range gi1-3
Switch(config-if-range)# lag 1 mode active
Switch# show lag
Load Balancing: src-dst-mac-ip.
Group ID | Type    |   Ports
---------+--------+--------------------------------
    1    |   LACP |  Inactive: gi1-3
    2    | ------ |
    3    | ------ |
    4    | ------ |
    5    | ------ |
    6    | ------ |
    7    | ------ |
    8    | ------ |
```

10.2. lag load-balance

Item	Description
Syntax	lag load-balance (src-dst-mac | src-dst-mac-ip)
	no lag load-balance
Parameter	**src-dst-mac:** Specify algorithm to balance traffic by using source and destination MAC address for all packets.
	src-dst-mac-ip: Specify algorithm to balance traffic by using source and destination IP address for IP packets and using source and destination MAC address for non-IP packets.
Default	Default load balance algorithm is src-dst-mac
Mode	Global Configuration
Usage	Link aggregation group port should transmit packets spread to all ports to balance traffic loading. There are two algorithm supported and this command allow you to select the algorithm.

Example:

This example shows how to change load balance algorithm to src-dst-mac-ip.

```
Switch(config)# lag load-balance src-dst-mac-ip
```

This example shows how to show current load balance algorithm.

```
Switch# show lag
Load Balancing: src-dst-mac-ip.

Group ID | Type |  Ports
---------+----------+-----------------------
    1    | --------- |
    2    | --------- |
    3    | --------- |
    4    | --------- |
    5    | --------- |
    6    | --------- |
    7    | --------- |
    8    | --------- |
```

10.3. lacp port-priority

Item	Description
Syntax	lacp port-priority <1-65535>
	no lacp port-priority

Parameter	**<1-65535>:** Specify port priority value
Default	Default port priority is 1.
Mode	Interface Configuration
Usage	LACP port priority is used for two connected DUT to select aggregation ports. Lower port priority value has higher priority. And the port with higher priority will be selected into LAG first. The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to configure interface GigabitEthernet1 lacp port priority to 100.

```
Switch(config)# interface Gi1
Switch(config-if)# lacp port-priority 100
```

10.4. lacp system-priority

Item	Description
Syntax	lacp system-priority <1-65535>
	no lacp system-priority
Parameter	**<1-65535>:** Specify system priority value
Default	Default system priority is 32768.
Mode	Global Configuration
Usage	LACP system priority is used for two connected DUT to select master switch.Lower system priority value has higher priority. And the DUT with higher priority can decide which ports are able to join the LAG. Use "**no lacp system-priority**" to restore to the default priority value. The only way to show this configuration is using "**show running-config**" command

Example:

This example shows how to configure lacp system priority to 1000.

```
Switch(config)# lacp system-priority 1000
```

10.5. lacp timeout

Item	Description
Syntax	lacp timeout (long | short)

	no lacp timeout
Parameter	**long**: Send LACP packet every 30 seconds.
	Short: Send LACP packet every 1 second.
Default	Default LACP timeout is long.
Mode	Interface Configuration
Usage	LACP need to send LACP packet to partner switch to check the link status. This command configure the interval of sending LACP packets. The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to configure interface Gi1 lacp timeout to short.

```
Switch(config)# interface Gi1
Switch(config-if)# lacp timeout short
```

10.6. show lacp

Item	Description
Syntax	show lacp sys-id
	show lacp [<1-8>] counters
	show lacp [<1-8>] (internal | neighbor) [detail]
	clear lacp [<1-8>] counters
Parameter	**[<1-8>]:** Specify the LAG id for the interface
	[detail]: Detailed internal information
Default	No default values for this command.
Mode	Privileged EXEC
Usage	Use "**show lacp sys-id**" command to displays the system identifier that is being used by LACP. The system identifier is made up of the LAPC system priority and the switch MAC address. Use "**show lacp counter**" command to display LACP statistic information. Use "**show lacp internal**" command to display local information. Use "**show lacp neighbor**" command to display remote information. State of the specific port. These are the allowed values: -—Port is in an unknown state. **bndl**—Port is attached to an aggregator and bundled with other ports. **susp**—Port is in a suspended state; it is not attached to any aggregator. **hot-sby**—Port is in a hot-standby state. **1indiv**—Port is incapable of bundling with any other port. **1indep**—Port is in an independent state (not bundled but able to switch data

	traffic. In this case, LACP is not running on the partner port). **down**—Port is down. State variables for the port, encoded as individual bits within a single octet with these meanings: bit0—LACP_Activity bit1—LACP_Timeout bit2—Aggregation bit3—Synchronization bit4—Collecting bit5—Distributing bit6—Defaulted bit7—Expired

Example:

This example shows how to show LACP statistics.

```
Switch# show lacp counters
           LACPDUs     LACPDUs
Port    Sent    Recv    Pkts Err
Channel group 1
gi1      0       0       0
gi2      0       0       0
```

This example shows how to show LACP local information.

```
Switch# show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
           F - Device is requesting Fast LACPDUs
           A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                        LACP port     Admin     Oper    Port        Port
Port    Flags   State     Priority      Key       Key    Number     State
gi1       FA      down      100          0x3e8     0x3e8   0x1         0x47
gi2       SA      down      1            0x3e8     0x3e8   0x2         0x45
gi3       SA      down      1            0x3e8     0x3e8   0x3         0x45
This example shows how to show LACP remote information.
Switch# show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs
             F - Device is sending Fast LACPDUs
             A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
```

```
                LACP port                       Admin  Oper   Port    Port
Port     Flags   Priority  Dev ID         Age    key    Key    Number State
gi1      FP      32768     0000.0000.0000  0s     0x3e8  0x3e8  0x1    0x56
gi2      FP      32768     0000.0000.0000  0s     0x3e8  0x3e8  0x2    0x56
gi3      FP      32768     0000.0000.0000  0s     0x3e8  0x3e8  0x3    0x56
```

10.7. show lag

Item	Description
Syntax	show lag
Parameter	
Default	No default values for this command.
Mode	Privileged EXEC
Usage	Use "**show lag**" command to show current LAG load balance algorithm and members active/inactive status.

Example:

This example shows how to show current LAG status.

```
Switch# show lag
Load Balancing: src-dst-mac-ip
Group ID | Type |  Ports
---------+------+----------------------
    1    |   LACP |  Inactive: gi1-3
    2    | ------ |
    3    | ------ |
    4    | ------ |
    5    | ------ |
    6    | ------ |
    7    | ------ |
    8    | ------ |
```

11. LLDP

11.1. clear lldp statistics

Item	Description
Syntax	clear lldp (global | interfaces LAG[<1-8>]|interfaces XGigabitEthernet[<1-4>]|interfaces GigabitEthernet[<1-24>]) statistics
Parameter	**[<1-8>]:** Specify the LAG id for the interface
Default	There is no default configuration for this command
Mode	Privileged EXEC
Usage	Use "**clear lldp statistics**" command to clear the LLDP RX/TX statistics.

Example:

This example shows how to clear LLDP statistics.

```
Switch# clear lldp global statistics
```

11.2. lldp

Item	Description
Syntax	lldp
	no lldp
Parameter	
Default	Default is enabled
Mode	Global Configuration
Usage	Use "**lldp**" command to enable LLDP RX/TX ability. The LLDP enable status is displayed by "**show lldp**" command. Use the **no** form of this command to disable the LLDP. When LLDP is disabled, the behavior of receiving LLDP PDU would be decided by "**lldp lldpdu**" command.

Example:

The following example sets LLDP enable/disable.

```
Switch (config)# lldp
Switch# show lldp

    State: Enabled
    Timer: 30 Seconds
    Hold multiplier: 4
```

```
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding

Port    |  State | Optional TLVs  | Address
--------+ ------ + -------------- + --------
    gi1 |  RX,TX |                |192.168.169.1
    gi2 |  RX,TX |                |192.168.169.1
    gi3 |  RX,TX |                |192.168.169.1
--More--
```

11.3. lldp rx

Item	Description
Syntax	lldp rx
	no lldp rx
Parameter	
Default	Default is enabled
Mode	Port Configuration
Usage	Use "**lldp rx**" command to enable the LLDP PDU RX ability. The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to disable the RX ability.

Example:

This example sets port gi1 to enable LLDP TX, port gi2 to disable RX but enable TX, port gi3 to enable RX but disable TX, port gi4 to disable RX and TX.

```
Switch(config)# interface gi1
Switch(config-if)# lldp rx
Switch(config-if)# lldp tx
Switch(config)# interface gi2
Switch(config-if)# no lldp rx
Switch(config-if)# lldp tx
Switch(config)# interface gi3
Switch(config-if)# lldp rx
Switch(config-if)# no lldp tx
Switch(config)# interface gi4
Switch(config-if)# no lldp rx
Switch(config-if)# no lldp tx
Switch(config-if)# end
Switch# show lldp interfaces gi1-4
```

```
State: Enabled Timer: 30 Seconds
Hold multiplier: 4 Reinit delay: 2 Seconds Tx delay: 2 Seconds
LLDP packet handling: Bridging
Port    |   State | Optional TLVs  | Address
--------+ ------ + -------------- + --------
    gi1 |   RX,TX |                |192.168.1.254
    gi2 |   TX    |                |192.168.1.254
    gi3 |   RX    |                |192.168.1.254
    gi4 | Disable |                |192.168.1.254
```

11.4. lldp tx-interval

Item	Description
Syntax	lldp tx-interval <5-32768>
	no lldp tx-interval
Parameter	**<5-32768>:** Specify the LLDP PDU TX interval in unit of second.
Default	Default TX interval is 30 seconds
Mode	Global Configuration
Usage	Use "**lldp tx-interval**" command to configure the LLDP TX interval. It should be noticed that both "**lldp tx-interval**" and "**lldp tx-delay**" affects the LLDP PDU TX time. The larger value of the two configurations decides the TX interval. The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to restore the interval to default value.

Example:

This example sets LLDP TX interval to 10 seconds.

```
Switch(config)# lldp tx-interval 10
Switch# show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

11.5. lldp reinit-delay

Item	Description
Syntax	lldp reinit-delay <1-10>
	no lldp reinit-delay
Parameter	**<1-10>:** Specify the LLDP re-initial delay time in unit of second.
Default	Default reinital delay is 2 seconds
Mode	Global Configuration
Usage	Use "**lldp reinit-delay**" to configure the LLDP re-initial delay. This delay avoids LLDP generate too many PDU if the port is up and down frequently. The delay starts to count when the port links down. The port would not generate LLDP PDU until the delay counts to zero. The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to restore the delay to default value.

Example:

This example sets LLDP re-initial delay to 5 seconds.

```
Switch(config)# lldp reinit-delay 5
Switch# show lldp

State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 5 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

11.6. lldp holdtime-multiplier

Item	Description
Syntax	lldp holdtime-multiplier <2-10>
	no holdtime-multiplier
Parameter	**<2-10>**: Specify the LLDP hold time multiplier.
Default	lldp holdtime-multiplier 4
Mode	Global Configuration
Usage	Use "**lldp holdtime-multiplier**" command to configure the LLDP PDU hold multiplier that decides time-to-live (TTL) value sent in LLDP advertisements: TTL = (tx-interval * holdtime-multiplier). The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to restore the multiplier to default value.

Example:

This example sets LLDP hold time multiplier to 3.

```
Switch(config)# lldp holdtime-multiplier 3
Switch# show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

11.7. lldp lldpdu

Item	Description
Syntax	lldp lldpdu (filtering|flooding|bridging)
Parameter	**filtering**:When LLDP is globally disabled, LLDP packets are bridging (bridging LLDP PDU to VLAN member ports).
	flooding:When LLDP is globally disabled, LLDP packets are filtered (deleted).
	bridging:When LLDP is globally disabled, LLDP packets are flooded (forwarded to all interfaces).
Default	Default LLDP PDU handling behavior when LLDP disabled is flooding
Mode	Global Configuration
Usage	Use "**lldp lldpdu**" command to configure the LLDP PDU handling behavior when LLDP is globally disabled. It should be noticed that if LLDP is globally enabled and per port LLDP RX status is configured to disabled, the received LLDP PDU would be dropped instead of taking the global disable behavior. The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to restore the behavior to default.

Example:

This example sets LLDP disable action to bridging.

```
Switch(config)# lldp lldpdu bridging
Switch# show lldp

State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
```

```
LLDP packet handling: Bridging
```

11.8. lldp tlv-select

Item	Description
Syntax	lldp tlv-select TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] no lldp tlv-select
Parameter	**TLV**: Specify the selected optional TLV. Available optional TLVs are : sys-name (system name), sys-desc (system description), sys-cap (system capability), mac-phy (802.3 MAC-PHY), lag (802.3 link aggregation), max- frame-size (802.3 max frame size), and management-addr (management address).
Default	Default is no selected optional TLV.
Mode	Port Configuration
Usage	Use "**lldp tlv-select**" command to attach selected TLV in PDU. The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to remove all selected TLV.

Example:

This example selects system name, system description, system capability,802.3 MAC-PHY, 802.3 link aggregation, 802.3 max frame size, and management address TLVs for interface gi1 and gi3.

```
Switch(config)# interface range gi 1,3
Switch(config-if-range)# lldp tlv-select port-desc sys-name sys-desc
sys-cap mac-phy lag max-frame-size management-addr
Switch(config-if-range)# end
Switch# show lldp interfaces gi1,3
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding

Port    |   State | Optional TLVs   | Address
--------+ ------ + -------------- + --------
    gi1 |   RX,TX | PD, SN, SD, SC |192.168.1.254
    gi3 |   RX,TX | PD, SN, SD, SC |192.168.1.254

Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size,
```

```
management-addr
802.1 optional TLVs
PVID: Enabled

Port ID: gi3
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size,
management-addr
802.1 optional TLVs
PVID: Enabled
```

11.9. lldp tlv-select pvid

Item	Description
Syntax	lldp tlv-select pvid (disable|enable)
	no lldp tlv-select pvid
Parameter	**disable:** Disable LLDP 802.1 PVID TLV attach state
	enable: Enable LLDP 802.1 PVID TLV attach state
Default	Default is enabled
Mode	Port Configuration
Usage	Use "**lldp tlv-select pvid**" command to configure the 802.1 PVID TLV attach enable status. The configuration could be shown by "show lldp" command. Use the **no** form of this command to restore the pvid to default value.

Example:

This example sets port gi1 PVID TLV attaches status to disable and port gi2 to enable.

```
Switch(config)# interface gi1
Switch(config-if)# lldp tlv-select pvid disable
Switch(config-if)# interface gi2
Switch(config-if)# lldp tlv-select pvid enable
Switch# show lldp interfaces gi1,gi2
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding

Port    |   State | Optional TLVs   | Address
--------+ ------ + -------------- + --------
    gi1 |   RX,TX |                 |192.168.1.254
    gi2 |   RX,TX | |               192.168.1.254
```

```
Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Disabled

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

11.10. lldp tlv-select vlan-name

Item	Description
Syntax	lldp tlv-select vlan-name (add|remove) VLAN-LIST
Parameter	**add VLAN-LIST:** Add VLAN list for LLDP 802.1 VLAN-NAME TLV on the specific interface. The configured ports should be member of all the specified VLANs or the VLAN-LIST is not valid.
	remove VLAN- LIST: Remove VLAN list of LLDP 802.1 VLAN-NAME TLV from interface.
Default	Default is no VLAN added.
Mode	Port Configuration
Usage	Use "**lldp tlv-select vlan-name**" command to add or remove VLAN list for 802.1 VLAN-NAME TLV. The configuration could be shown by "**show lldp**" command.

Example:

This example add VLAN 100 to VLAN-NAME TLV for port gi10.

```
Switch(config)# vlan 100
Switch(config-vlan)# exit
Switch(config)# interface gi1
Switch(config-if)# switchport trunk allowed vlan add all
Switch(config-if)# lldp tlv-select vlan-name add 100
Switch(config-if)# end
Switch# show lldp interfaces gi1

State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

```
Port    |   State | Optional TLVs  | Address
--------+ ------ + -------------- + --------
    gi1 |   RX,TX |                |192.168.1.2
Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
VLANs: 100
```

11.11. lldp tx

Item	Description
Syntax	lldp tx
	no lldp tx
Parameter	
Default	Default is enabled
Mode	Port Configuration
Usage	Use "**lldp tx**" command to enable the LLDP PDU TX ability. The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to disable the TX ability.

Example:

This example sets port gi1 to enable LLDP TX, port gi2 to disable RX but enable TX, port gi3 to enable RX but disable TX, port gi4 to disable RX and TX.

```
Switch(config)# interface gi1
Switch(config-if)# lldp rx
Switch(config-if)# lldp tx
Switch(config)# interface gi2
Switch(config-if)# no lldp rx
Switch(config-if)# lldp tx
Switch(config)# interface gi3
Switch(config-if)# lldp rx
Switch(config-if)# no lldp tx
Switch(config)# interface gi4
Switch(config-if)# no lldp rx
Switch(config-if)# no lldp tx
Switch(config-if)# end
Switch# show lldp interfaces gi1-4
State: Enabled
Timer: 30 Seconds
```

```
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging
Port    |   State | Optional TLVs  | Address
--------+ ------ + -------------- + --------
    gi1 |   RX,TX |                |192.168.1.254
    gi2 |   TX    |                |192.168.1.254
    gi3 |   RX    |                |192.168.1.254
    gi4 |Disable |                 |192.168.1.254
```

11.12. lldp tx-delay

Item	Description
Syntax	lldp tx-delay <1-8192>
	no lldp tx-delay
Parameter	**<1-8192>:** Specify the LLDP tx delay in unit of seconds.
Default	Default TX delay is 2 seconds
Mode	Global Configuration
Usage	Use "**lldp tx-delay**" command to configure the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case LLDP PDU is sent such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown by "**show lldp**" command. Use the **no** form of this command to restore the delay to default value.

Example:

This example sets LLDP PDU TX delay to 10 seconds.

```
Switch(config)# lldp tx-delay 10
Switch# show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 10 Seconds
LLDP packet handling: Flooding
```

11.13. lldp med

Item	Description

Syntax	lldp med no lldp med
Parameter	
Default	Default is enabled
Mode	Interface Configuration
Usage	Use "**lldp med**" command to enable the LLDP med capabilities. The configuration could be shown by "**show lldp med**" command. Use the **no** form of this command to disable the med capabilities.

Example:

The following example sets LLDP med enable/disable.

```
Switch(config-if)# lldp med
Switch# show lldp med
 Fast Start Repeat Count: 3
 lldp med network-policy voice: manual

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |       No |        No |     N/A
    gi2 |           No |            Yes |       No |        No |     N/A
```

11.14. lldp med tlv-select

Item	Description
Syntax	lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV] no lldp med tlv-select
Parameter	**MEDTLV:**LLDP MED optional TLV (network-policy, location, inventory)
Default	Default is enable the network-policy
Mode	Interface Configuration
Usage	Use "**lldp med tlv-select**" command to enable the LLDP med network-policy, location, inventory. The configuration could be shown by "**show lldp med**" command. Use the **no** form of this command to disable the med MEDTLV.

Example:

The following example sets LLDP med tlv-select enable/disable.

```
Switch(config-if)# lldp med tlv-select location
```

11.15. lldp med fast-start-repeat-count

Item	Description
Syntax	lldp med fast-start-repeat-count <1-10>
	no lldp med fast-start-repeat-count
Parameter	**<1-10>**：Configure LLDP MED fast start repeat count
Default	Default is 3
Mode	Global Configuration
Usage	Use "**lldp med fast-start-repeat-count**" command to LLDP MED fast repeat count set. The configuration could be shown by "**show lldp med**" command. Use the **no** form of this command to default setting.

Example:

The following example sets LLDP med ast repeat count set.

```
Switch(config)# lldp med fast-start-repeat-count 2
```

11.16. lldp med network-policy(global)

Item	Description
Syntax	lldp med network-policy <1-32> app (voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice|video-conferencing|streaming-video|video-signaling) vlan <1-4094> vlan-type (tag|untag) priority <0-7> dscp <0-63>
	no lldp med network-policy <1-32>
Parameter	**<1-32>:** Network policy index
	<1-4094>:Specify the VLAN ID
	<0-7>:Specify the priority values
	<0-63>:Specify the dscp values
Default	
Mode	Global Configuration
Usage	Use "**lldp med network-policy app vlan vlan-type priority dscp**" command to LLDP MED network policy set. The configuration could be shown by "**show lldp med**" command. Use the **no** form of this command to default setting.

Example:

The following example sets LLDP med network-policy set.

```
Switch(config)# lldp med network-policy 2 app guest-voice vlan 1 vlan-type
```

```
tag priority 1 dscp 2
```

11.17. lldp med network-policy(interface)

Item	Description
Syntax	lldp med network-policy (add|remove) IDX_LIST
Parameter	**add:** Add network policy to port binding
	remove: Remove network policy to port binding
	IDX_LIST:Network policy index list, index range is 1-32, ex: 1,30-32
Default	
Mode	interface Configuration
Usage	Use "**lldp med network-policy** " command to Add/remove LLDP MED network policy binding over ports. The configuration could be shown by "**show lldp med**" command.

Example:

The following example sets Add LLDP MED network policy binding over ports.

```
Switch(config-if)# lldp med network-policy add 3
```

11.18. lldp med location

Item	Description
Syntax	lldp med location (coordinate|civic-address|ecs-elin) ADDR
	no lldp med location (coordinate|civic-address|ecs-elin)
Parameter	**coordinate:** The location is specified as coordinates. Range: 16 hexadecimal bytes exactly.
	civic-address: The location is specified as civic address. Range: 6 to 160 hexadecimal bytes.
	ecs-elin:The location is specified as ECS ELIN. Range: 10 to 25 hexadecimal bytes.
Default	
Mode	interface Configuration
Usage	Use "**lldp med location** " command to LLDP MED location set. The configuration could be shown by "**show lldp med**" command.

Example:

The following example sets LLDP MED location.

```
Switch(config-if)# lldp med location coordinate
1122AB11223344556677889977 88aabb
```

11.19. show lldp

Item	Description
Syntax	show lldp show lldp interface IF_NMLPORTS
Parameter	**IF_NMLPORTS:** Specify the ports to display information
Default	This command has no default value.
Mode	Privileged EXEC
Usage	Use "**show lldp**" and "**show lldp interface**" commands to display LLDP global information including LLDP enable status, LLDP PDU TX interval, hold time multiplier, re-initial delay, TX delay, and LLDP packet handling when LLDP is disabled. The per port information displayed includes port LLDP RX/TX enable status, selected TLV to TX and IP address. The abbreviations in optional TLVs are: port description (PD), system name (SN), system description (SD), and system capability (SC).

Example:

This example displays lldp information of port gi1 and gi2

```
Switch# show lldp interfaces gi1,gi2
State: Disabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding

Port    |   State | Optional TLVs   | Address
--------+ ------ + -------------- + --------
    gi1 |   RX,TX | PD, SN, SD, SC |192.168.1.254
    gi1 |   RX,TX |                |192.168.1.254

Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max- frame-size,
management-addr
802.1 optional TLVs
PVID: Enabled

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

11.20. show lldp local-device

Item	Description
Syntax	show lldp local-device show lldp interfaces IF_NMLPORTS local-device
Parameter	**IF_NMLPORTS:** Specify the ports to display information
Default	There is no default configuration for this command
Mode	Privileged EXEC
Usage	Use "**show lldp local-device**" command to show the local configuration of LLDP PDU. By the commands, a user can view the contents of LLDP/ LLDP- MED TLVs that would be attached in LLDP PDU.

Example:

This example displays the local device information.

```
Switch# show lldp local-device
LLDP Local Device Information:
  Chassis Type : Mac Address
  Chassis ID   : 00:E0:4C:00:00:00
  System Name  : Switch
  System Description  : TS928F
  System Capabilities Support : Bridge
  System Capabilities Enable  : Bridge
  Management Address : 192.168.169.1(IPv4)
  Management Address : fe80::2e0:4cff:fe00:0(IPv6)
Switch(config)# show lldp interfaces gi1 local-device
Device ID: 00:E0:4C:00:00:00
Port ID: gi1
System Name: Switch
Capabilities: Bridge
System description: TS928F
Port description:
Management address: 192.168.169.1
Management address: fe80::2e0:4cff:fe00:0
Time To Live: 30
802.3 MAC/PHY Configur/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 10BASE-T  full duplex,
100BASE-TX full duplex, 1000BASE-T full duplex
Operational MAU type: Other or unknown
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
```

```
Aggregation status: Not currently in aggregation
Aggregation port ID: 0
802.3 Maximum Frame Size: 1518
802.1 VLAN: 100
802.1 VLAN name: 100(VLAN0100)
```

11.21. show lldp med

Item	Description
Syntax	show lldp med
	show lldp interfaces IF_NMLPORTS med
Parameter	**IF_NMLPORTS:** Specify the ports to display information
Default	There is no default configuration for this command
Mode	Privileged EXEC
Usage	Use "**show lldp med**" command to display the LLDP MED configuration information.

Example:

This example display the LLDP MED information.

```
Switch# show lldp med
 Fast Start Repeat Count: 3
 lldp med network-policy voice: manual
Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |           No |            Yes |       No |        No |     N/A
    gi2 |           No |            Yes |       No |        No |     N/A
    gi3 |           No |            Yes |       No |        No |     N/A
    gi4 |           No |            Yes |       No |        No |     N/A
--More-
Switch# show lldp interfaces gi1 med

Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
------ + ------------ + -------------- + -------- + --------- + -------
   gi1 |           No |            Yes |       No |        No |     N/A

Port ID: gi1
Network policies:
```

11.22. show lldp neighbor

Item	Description
Syntax	show lldp neighbor show lldp interfaces IF_NMLPORTS neighbor
Parameter	**IF_NMLPORTS:** Specify the ports to display information
Default	There is no default configuration for this command
Mode	Privileged EXEC
Usage	Use "**show lldp neighbor**" command to display the received neighbor LLDP PDU information. When LLDP PDU is received on LLDP RX enable ports, system would store the PDU information in database until time to live of the PDU counts down to zero.

Example:

This example displays the neighbor information.

```
Switch# show lldp neighbor
 Port |   Device ID    |    Port ID    |   SysName    | Capabilities  | TTL
 ---- + -------------+ ----------- + ---------------+ ------------- + -----
 gi24 | 00:1B:21:22:33:81 |00:1B:21:22:33:81 |      |             |  3326
```

11.23. show lldp statistics

Item	Description
Syntax	show lldp statistics show lldp interfaces IF_NMLPORTS statistics
Parameter	**IF_NMLPORTS:** Specify the ports to display information
Default	There is no default configuration for this command
Mode	Privileged EXEC
Usage	Use "**show lldp statistics**" command to display the LLDP RX/TX statistics.

Example:

This example display the LLDP statistics.

```
Switch# show lldp statistics
LLDP Global Statistics:
Insertions : 0
Deletions  : 0
Drops      : 0
Age Outs   : 0

| TX Frames |          RX Frames       |         RX TLVs             | RX Ageouts
```

```
Port|   Total   | Total | Discarded | Errors | Discarded | Unrecognized |    Total
----+---------+-------+---------+--------+----------+-------------+--------
gi1 |        0 |      0 |        0 |      0 |        0 |           0 |        0
gi2 |        0 |      0 |        0 |      0 |        0 |           0 |        0
gi3 |        0 |      0 |        0 |      0 |        0 |           0 |        0
gi4 |        0 |      0 |        0 |      0 |        0 |           0 |        0
gi5 |        0 |      0 |        0 |      0 |        0 |           0 |        0
gi6 |        0 |      0 |        0 |      0 |        0 |           0 |        0
    --More--
    Switch(config)# show lldp interfaces gi1 statistics

    LLDP Port Statistics:
      | TX Frames |       RX Frames          |         RX TLVs         | RX Ageouts
Port  | Total    | Total | Discarded | Errors | Discarded | Unrecognized |   Total
------+--------+------+----------+-------+----------+-------------+-----
gi1   |      0 |     0 |      0    |    0   |      0   |          0   |     0
```

11.24. show lldp tlv-overloading

Item	Description
Syntax	show lldp interfaces IF_NMLPORTS tlvs-overloading
Parameter	**IF_NMLPORTS:** Specify the ports to display information
Default	There is no default configuration for this command
Mode	Privileged EXEC
Usage	The LLDP PDU is composed by TLVs and selected number TLVs may compose a large PDU that the system can not handle. The maximum PDU length is to take the smaller number of jumbo frame size minus 30 bytes (30 bytes kept for header) or 1488 bytes. Use "**show lldp interfaces gi1 tlvs-overloading**" command to display the length of LLDP TLVs and if the TLVs overload the PDU length. The TLVs with status marked "overload" would not be transmitted.

Example:

This example display the LLDP TLVs overloading status of port gi1.

```
Switch# show lldp interfaces gi1 tlvs-overloading

gi1:

    TLVs Group          |  Bytes  |     Status
-----------------------+--------+----------------
           Mandatory    |     21 |    Transmitted
```

```
           802.3       |      30 |    Transmitted
            Optional   |     128 |    Transmitted
Total: 179 bytes
Left: 1309 bytes
```

12. Logging

12.1. clear logging

Item	Description
Syntax	show lldp interfaces IF_NMLPORTS tlvs-overloading
Parameter	**IF_NMLPORTS:** Specify the ports to display information
Default	N/A
Mode	Privileged EXEC
Usage	To clear the log messages from the internal logging buffer and flash, use the command clear logging in the Privileged EXEC mode.

Example:

The following example clear the log messages stored in RAM and Flash.

```
Switch# clear logging buffered
Switch# clear logging file
```

12.2. logging

Item	Description
Syntax	logging
	no logging
Parameter	
Default	Logging service is enabled.
Mode	Global Configuration
Usage	To enable logging service on the switch, use the command **logging** in the Global Configuration mode. Otherwise, use the **no** form of the command to disable the logging service on the switch. The status of global logging server is available from the command **show logging** in the Privileged EXEC mode. When the logging service is enabled, logging on and off at each destination rule can be individually configured by the command **logging console**, **logging buffered**, **logging file**, and **logging host** in the Global Configuration mode. If the logging service is disabled, no messages will be sent to these destinations.

Example:

The following example disables and enables the logging service on the switch.

```
Switch(config)# no logging
Switch(config)# logging
```

12.3. logging host

Item	Description
Syntax	logging host (ip-addr|hostname) [facility facility] [port port] [severity sev]
	no logging host (ip-addr|hostname)
Parameter	**ipv4-addr:** IPv4 address of the remote logging server.
	hostname: Hostname of the remote logging server.
	acility facility**:** Specify the facility of the logging messages. It can be on of the following value: local0, local1, local2, local3, local4, local5, local6, and local7. The default value of facility is local7.
	port port**:** Specify the port number of the remote logging server.The valid range is from 0 to 65535, and the default value is 512.
	severity sev**:** Specify the minimum severity of the logging messages.The valid range is from 0 to 7, and the number 0 to 7 represents emerg, alert, critical, error, warning, notice, info, and debug individually. The default value of minimum severity level is 5 (emerg, alert, crit, error,warning, notice).
Default	No remote logging destination is configured.
Mode	Global Configuration
Usage	To define the logging server, use the command **logging host** to add the remote logging server in the Global Configuration mode. Otherwise, use the command **no logging host** to remove the remote logging rules. For the host name configuration, logging service would try translating the host name to IP address directly. Add the logging host would be failed on the failure of host name translating.

Example:

The following example adds the remote logging rules by IP and Hostname.

```
Switch(config)# logging host 1.2.3.4
Switch(config)# logging host SYSLOG
```

12.4. logging severity

Item	Description
Syntax	logging (buffered|console|file) [severity sev]
	no logging (buffered|console|file)
Parameter	**buffered:** Log messages to RAM.
	console: Log messages to console buffer.

	file：Log messages to Flash.
	severity sev: Specify the minimum severity of the logging messages.The valid range is from 0 to 7, and the number 0 to 7 represents emerg, alert, critical, error, warning, notice, info, and debug individually. The default minimum severity of the logging severity configuration is 5(emerg, alert, crit, error, warning, notice).
Default	Logging to buffered and console is enabled, and the default minimum severity level is 5 (emerg, alert, crit, error, warning, notice)
Mode	Global Configuration
Usage	To set the minimum severity for the messages that are logged to RAM, console, or Flash, use the command logging severity in the Global Configuration mode. Use the **no** form of the command to remove the mechanism of logging to RAM, console, or Flash individually.

Example:

The following example sets the minimum severity level of logging to RAM and Flash as debugging.

```
Switch(config)# logging buffered severity 7
Switch(config)# logging file severity 7
```

12.5. show logging

Item	Description
Syntax	show logging [buffered|file]
Parameter	**buffered:** Display the log messages stored in the RAM.
	file: Display the log messages stored in the Flash.
Default	
Mode	Previledged EXEC
Usage	To display the global logging configuration, and the logging messages stored in the RAM and Flash, use the command **show logging** in the Privileged EXEC mode.

Example:

The following example shows the global logging configuration.

```
Switch# show logging Logging service is enabled

TARGET  |  STATUS  |     Server (PORT) | FACILITY | LOG LEVEL
--------+----------+-------------------+----------+-----------------
buffered|  enabled |                   |          |emerg, alert, crit, error,
                                                    warning, notice, info,
                                                  debug
```

```
console |  enabled |                  |         |emerg, alert, crit, error,
                                                  warning, notice
file | disabled |                    |         |
host |  enabled |       1.2.3.4(  514)|  local7  |emerg, alert, crit, error,
                                                  warning, notice
```

The following table describes the significant fields shown in the example:

Field	Description
TARGET	**The destinations where the logging messages are stored.**
STATUS	**The status of logging destinations.**
Server (PORT)	**Server address and port number for the remote logging.**
FACILITY	**The facility of the log messages.**
LOG LEVEL	**The severity level of the log messages.**

The following example shows the log messages stored in the RAM.

```
Switch# show logging buffered
Log messages in buffered
NO.|    Timestamp   |   Category    | Severity |   Message
---+---------------+----------+-------------+-------------------------
1|Jan 01 2000 08:14:47|    AAA|    notice| New console connection for user
                                          admin, source async    ACCEPTED
2|Jan 01 2000 08:03:12|    AAA|    notice| New console connection for user
                                          admin, source async    ACCEPTED
3|Jan 01 2000 08:01:13|    System| notice| System Startup!
4|Jan 01 2000 08:01:13|    System| notice| Logging is enabled
```

The following table describes the significant fields shown in the example:

Field	Description
NO	**The number of log entry.**
Timestamp	**Time when the message was generated.**
Category	**The category of the message.**
Severity	**The severity level of the messages.**
Message	**The message content.**

13. MAC Address Table

13.1. clear mac address-table

Item	Description
Syntax	clear mac address-table dynamic [interfaces IF_PORTS|vlan vlan-id]
Parameter	**Interfaces IF_PORTS:** Delete all dynamic addresses learned on the specific interface.
	vlan vlan-id: Delete all source addresses learned on the specific VLAN.
Default	
Mode	Previledged EXEC
Usage	To clear the dynamic (learned) MAC entries from the MAC address table, the specific interface, or the specific VLAN, use the command **clear mac address-table** in the Priveleged EXEC mode.

Example:

The following example clears the learned MAC addresses on the interface gi1.

```
Switch# clear mac address-table dynamic interfaces gi1
```

13.2. mac address-table aging-time

Item	Description
Syntax	mac accress-table aging-time seconds
Parameter	**seconds:** The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds,and the default value is 300 seconds.
Default	The default aging time is 300 seconds.
Mode	Global Configuration
Usage	To set the aging time of the MAC address table, use the command **mac address-table aging-time** in the Global Configuration mode.

Example:

The following example set the agimg time to 500 seconds.

```
Switch(config)# mac address-table aging-time 500
```

13.3. mac address-table static

Item	Description
Syntax	mac address-table static mac-addr vlan vlan-id interfaces IF_PORTS
	mac address-table static mac-addr vlan vlan-id drop
	no mac address-table static mac-addr vlan vlan-id
Parameter	**mac-addr:** MAC address.
	vlan *vlan-id*: Specify the VLAN ID for the interface
	Interface IF_PORTS: Specify the interface ID or a list of interface IDs.
	drop: Drop the packets with the specified source or destination unicast MAC address.
Default	No static addresses are configured
Mode	Global Configuration
Usage	To add a static address to the MAC address table, use the command **mac address-table static** in the Global Configuration mode. For the unicast MAC address filtering, use the command **mac address-table static** with parameter **drop** to drop the packets with the specified source or destination unist MAC address. To delete the static entry from the MAC address table, use the **no** form of the command

Example:

The following example adds a static address into MAC address table.

```
Switch(config)# mac address-table static 00:11:22:33:44:55 vlan 1
interfaces gi5
```

The following example adds a rule of unist address filtering into MAC address table.

```
Switch(config)# mac address-table static 00:11:22:33:44:55 vlan 1 drop
```

13.4. show mac address-table

Item	Description
Syntax	show mac address-table [dynamic|static] [interface IF_PORTS] [vlan vlan-id]
	show mac address-table [vlan <1-4094>] [interfaces IF_PORTS]
	show mac address-table [mac-addr] [vlan vlan-id]
Parameter	**dynamic** : Display only dynamic MAC addresses
	static: Display only static MAC addresses
	Interface IF_PORTS: Display the MAC addresses entries for a specifc interface.
	vlan vlan-id: Display the MAC address entries for a specific VLAN.

	mac-addr: Display entries for a specific MAC address
Default	
Mode	Privileged EXEC
Usage	To show the entry in the MAC address table, use the command **show mac address-table** in the Privilieged EXEC mode.

Example:

The following example displays the entire MAC addrss table.

```
Switch# show mac address-table
 VID  |    MAC Address     |       Type        |   Ports
-----+-------------------+---------------+-----------
   1 | 00:E0:4C:00:00:00 |    Management    | CPU
   1 | 00:11:22:33:44:55 |       Static      | gi5
   1 | 00:11:22:33:44:56 |       Static      | Drop
   1 | 00:1B:21:22:33:81 |      Dynamic      | gi24

Total number of entries: 4
```

The following example displays the static MAC address configuration for the interface GigabitEthernet1.

```
Switch# show mac address-table static interfaces Gi1

 VID  |    MAC Address    |       Type        |   Ports
------+-------------------+-------------------+---------------
    1 | 00:11:22:33:44:56 |       Static      | Drop

Total number of entries: 1
```

The following example displays address table entries containing the specified MAC address.

```
Switch# show mac address-table 00:11:22:33:44:55 vlan 100
VID |   MAC Address     |   Type    |   Ports
----+-----------------+-----------+---------------
100 | 00:11:22:33:44:55 |  Static  | gi1

 Total number of entries: 1
```

13.5. show mac address-table counters

Item	Description
Syntax	show mac address-table counters
Parameter	

Default	
Mode	Privileged EXEC
Usage	To display the total entries in the MAC addrss table, use the command **show mac address-table counters** in the Privilieged EXEC mode.

Example:

The following example display numbers of addresses in the address table.

```
Switch# show mac address-table counters
 Total number of entries: 5
```

13.6. show mac address-table aging-time

Item	Description
Syntax	show mac address-table aging-time
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show MAC address aging time, use the command show **mac address-table aging-time** in the Privilieged EXEC mode.

Example:

The following example displays aging time for the MAC address table.

```
Switch# show mac address-table aging-time
 Mac Address Table aging time: 300 sec
```

14. MAC VLAN

14.1. vlan mac-vlan group (Global)

Item	Description
Syntax	vlan mac-vlan group <1- 2147483647> mac-address mask <9-48>
	no vlan mac-vlan group mac-address mask <9-48>
Parameter	**<1-2147483647>:** Specify the group ID
	mac-address: Specify the MAC address to be mapped.
	<9-48>: Specify the mask length of MAC address.
Default	No MAC Groups are configured.
Mode	Global Configuration
Usage	Use the "**vlan mac-vlan group**" command to create MAC address group. Use the **no** form of this command to delete specify group.

Example:

The following example shows how to create a MAC group with group ID 3.

```
Switch(config)# vlan mac-vlan group 333 22:33:44:55:66:77 mask 48
```

14.2. vlan mac-vlan group (Interface)

Item	Description
Syntax	vlan mac-vlan group <1- 2147483647> vlan <1-4094>
	no vlan mac-vlan [group <1- 2147483647>]
Parameter	**<1-2147483647>:** Specify the group ID.(optional in no form) Delete all mapping group if not specify.
	<1-4094>: Specify the VLAN ID to give to match packet.
Default	No mappings are configured.
Mode	Interface Configuration
Usage	Use the "**vlan mac-vlan group**" to create mapping of group and VLAN ID of an interface. Use the **no** form of this command to delete mapping.

Example:

The following example shows how to mapping group id 333 to VLAN 100 on interface GigabitEthernet1.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)#vlan mac-vlan group 333 vlan 100
```

14.3. show vlan mac-vlan groups

Item	Description
Syntax	show vlan mac-vlan groups
Parameter	
Default	
Mode	Privileged EXEC
Usage	Use the **show vlan mac-vlan groups** command to display mac groups configuration

Example:

This following example shows how to display mac group.

```
Switch# show vlan mac-vlan groups

  Mac Address    Mask   Group Id
---------------- ---------- ------------
22:33:44:55:66:77   48         333

Total 1 Entry
```

14.4. show vlan mac-vlan interfaces

Item	Description
Syntax	show vlan mac-vlan [interfaces IF_PORTS]
Parameter	**IF_PORTS:** (Optional) Specify interfaces mac vlan to display.Display all ports if not specify.
Default	
Mode	Privileged EXEC
Usage	Use the **show vlan mac-vlan interface** command in EXEC mode to display the mac-vlan interfaces setting

Example:

The following example shows how to display the MAC-Based VLAN interfaces setting

```
Switch# show vlan mac-vlan interfaces Gi1

Interface gi1 Mac based VLANs:
  Group ID    Vlan ID
------------     -------
```

15. Management ACL

15.1. management access-list

Item	Description
Syntax	management access-list NAME
	no management access-list NAME
Parameter	**NAME:** The name of management ACL
Default	No management ACL is configured.
Mode	Global Configuration
Usage	Use the **management access-list** command to create a management access list and to enter management access-list configuration mode. The name of ACL must be unique that cannot have same name with other management ACL. Use the **no** form of this command to delete.

Example:

The following example shows how to add a management ACL with name "test".

```
Switch(config)# management access-list test
```

15.2. management access-class

Item	Description
Syntax	management access-class NAME
	no management access-class
Parameter	**NAME:** The name of management ACL to be used.
Default	Default is no management ACL restrictions
Mode	Global Configuration
Usage	Use the **management access-class** command to activate a management ACL. Use the **no** form of this command to delete.

Example:

The following example shows how to add a management ACL with name "test".

```
Switch(config)# management access-class test
```

15.3. deny

Item	Description
Syntax	[sequence <1-65535>] deny interfaces IF_PORTS service

	(all|http|https|snmp|ssh|telnet)
	[sequence <1-65535>] deny ip A.B.C.D/A.B.C.D interfaces IF_PORTS service (all|http|https|snmp|ssh|telnet)
	[sequence <1-65535>] deny ipv6 X:X::X:X/<0-128> interfaces IF_PORTS service (all|http|https|snmp|ssh|telnet)
Parameter	**<1-65535>**: (Optional) Specify sequence index of ACL entry, the sequence index represent the priority of an entry in ACL. If not specified, the switch assigns a number from 1 in ascending order.
	interfaces IF_PORTS: Specify the interface ID or a list of interface IDs.
	ip A.B.C.D/A.B.C.D: Specify the source IP address and mask of packet.
	ipv6 X:X::X:X/<0-128>: Specify the source IPv6 address and prefix length of packet.
	(all|http|https|snmp|ssh|telnet): Specify the type of services.
Default	No rules are configured.
Mode	Management Access-List Configuration
Usage	Use the deny command to add deny rules that drop those packets hit the rule.

Example:

The following example shows how to add a deny rule to drop all types of services packets that source ip is 1.1.1.1 from interface gi1.

```
Switch(config)# management access-list test
Switch(config-macl)# sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi1 service all
```

15.4. permit

Item	Description
Syntax	[sequence <1-65535>] permit interfaces IF_PORTS service (all|http|https|snmp|ssh|telnet)
	[sequence <1-65535>] permit ip A.B.C.D/A.B.C.D interfaces IF_PORTS service (all|http|https|snmp|ssh|telnet)
	[sequence <1-65535>] permit ipv6 X:X::X:X/<0-128> interfaces IF_PORTS service (all|http|https|snmp|ssh|telnet)
Parameter	**<1-65535>:** (Optional) Specify sequence index of ACL entry, the sequence index represent the priority of an entry in ACL. If not specified, the switch assigns a number from 1 in ascending order.
	interfaces IF_PORTS: Specify the interface ID or a list of interface IDs.
	ip A.B.C.D/A.B.C.D: Specify the source IP address and mask of packet.
	ipv6 X:X::X:X/<0-128>: Specify the source IPv6 address and prefix length of packet.
	(all|http|https|snmp|ssh|telnet): Specify the type of services.
Default	No rules are configured.

Mode	Management Access-List Configuration
Usage	Use the permit command to add permit rules that bypass those packets hit the rule.

Example:

The following example shows how to add a permit rule to bypass http service packets that source ip is 2.2.2.2 from interface gi1.

```
Switch(config)# management access-list test
Switch(config-macl)# sequence 2 permit ip 2.2.2.2/255.255.255.255
interfaces gi1 service http
```

15.5. no sequence

Item	Description
Syntax	no sequence <1-65535>
Parameter	<1-65535> Specify sequence index of ACL entry to delete.
Default	No rules are configured.
Mode	Management Access-List Configuration
Usage	Use the **no sequence** command to delete an entry in management ACL.

Example:

The following example shows how to delete an entry.

```
Switch(config)# management access-list test
Switch(config-macl)# sequence 10 deny interfaces gi1 service all
Switch(config-macl)# no sequence 10
```

15.6. show management access-class

Item	Description
Syntax	show management access-class
Parameter	
Default	No default is defined.
Mode	Privileged EXEC
Usage	Use the **show management access-class** command to show the active management access-list.

Example:

The example shows how to show management access-class

```
Switch# show management access-class
  Management access-class is enabled, using access-list test
```

15.7. show management access-list

Item	Description
Syntax	show management access-list [NAME]
Parameter	NAME Specify the name of management ACL to displayed
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show management access-lis**t command to show management ACL.

Example:

The example shows how to show management access-list

```
Switch# show management access-list
1 management access-list is created
test
----
sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi1 service all
    ! (Note: all other access implicitly denied)
```

16. Mirror

16.1. mirror session destination interface

Item	Description
Syntax	mirror session <1-4> destination interface IF_NMLPORT [allow-ingress]
	no mirror session <1-4> destination interface IF_NMLPORT
	no mirror session (<1-4> | all)
Parameter	**<1-4>:** Specify the mirror session to configure
	IF_NMLPORT: Specify the SPAN destination. A destination must be a physical por
	allow-ingress: Enable ingress traffic forwarding.
Default	No monitor sessions are configured.
Mode	Global Configuration
Usage	Use the "**mirror session destination interface**" command to start a destination interface of a port mirror session. Use the **no** form of this command to stop a destination interface of a port mirroring session. Use the "**no mirror session**" command to disable all mirror sessions or specific mirror session.

Example:

The following example shows how to create a local session 1 to monitor both sent and received traffic on source port gi1.

```
Switch(config)# mirror session 1 destination interface GigabitEthernet1
Switch# show mirror session 1
Session 1 Configuration
Source RX Port  : gi2-5
Source TX Port  : gi2-5
Destination port    : gi1
Ingress State: disabled
```

16.2. mirror session source interface

Item	Description
Syntax	mirror session <1-4> source interfaces IF_PORTS (both | rx | tx)
	no mirror session <1-4> source interfaces IF_PORTS (both | rx | tx)
	no mirror session (<1-4> | all)
Parameter	**<1-4>:** Specify the mirror session to configure
	IF_PORTS: Specify the source interface, Valid interfaces include physical

	ports and port channels.
	both: Mirror tx and rx direction.
	rx: Mirror rx direction only.
	tx: Mirror trx direction only.
Default	No monitor sessions are configured.
Mode	Global Configuration
Usage	Use the "**mirror session source interface**" command to start a port mirror session. Use the **no** form of this command to stop a port mirroring session. Use the "**no mirror session**" command to disable all mirror sessions or specific mirror session.

Example:

The following example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port gi1.

```
Switch(config)# mirror session 1 source interface GigabitEthernet2-5 both
Switch(config)# mirror session 1 destination interface GigabitEthernet1
Switch(config)# show mirror session 1
Session 1 Configuration
Source RX Port  : gi2-5
Source TX Port  : gi2-5
Destination port   : gi1
Ingress State: disabled
```

16.3. show mirror

Item	Description
Syntax	show mirror [session <1-4>]
Parameter	**<1-4>:** Specify the mirror session to display
Default	
Mode	Privileged EXEC
Usage	Use the **show mirror** command to display mirror session configuration

Example:

This following example shows how to display mirror session configuration

```
Switch(config)# show mirror
Session 1 Configuration
Source RX Port    : gi2-5
Source TX Port    : gi2-5
Destination port  : gi1
Ingress State: disabled

Session 2 Configuration
```

```
Mirrored source   : Not Config
Destination port  : Not Config

Session 3 Configuration
Mirrored source   : Not Config
Destination port  : Not Config

Session 4 Configuration
Mirrored source   : Not Config
Destination port  : Not Config
```

17. MVR

17.1. Mvr

Item	Description
Syntax	mvr no mvr
Parameter	
Default	Default is disabled
Mode	Global Configuration
Usage	Use the **mvr** command to enable MVR function. The command will clear all mvr VLAN ID multicast snooping group. Use the **no** form of this command to disable. Disable will clear all mvr group. You can verify settings by the **show mvr** command.

Example:

The following example specifies that set mvr test.

```
Switch(config)# mvr
Switch(config)# no mvr
Switch# show mvr
MVR Running : Disabled
MVR Multicast VLAN : 1
MVR Group Range : None
MVR Max Multicast Groups : 128
MVR Current Multicast Groups : 0
MVR Global query response time : 1 sec
MVR Mode : compatible
```

17.2. mvr vlan

Item	Description
Syntax	mvr vlan <VLAN-ID>
Parameter	**<VLAN-ID>:** The exist static vlan id
Default	Default mvr vlan id is 1
Mode	Global Configuration
Usage	Use the **mvr vlan** command to modify mvr vlan id when the mvr status is enabled. Change mvr vlan id will delete the old mvr vlan and new mvr vlan group. If there have configure source or receiver port, there will check the source

	must only in the mvr vlan , and receiver port must not in the mvr vlan member. You can verify settings by the **show mvr** command.

Example:

The following example specifies that configure mvr vlan 2 test.

```
Switch(config)# vlan 2
Switch(config)# mvr
The operation will delete groups of VLAN ID is MVR VLAN include static groups.
Continue? [yes/no]:y
Switch(config)# mvr vlan 2
The operation will delete the old and new MVR VLAN groups include static
MVR groups.Continue? [yes/no]:y
Switch# show mvr
MVR Running : Enabled
MVR Multicast VLAN : 2
MVR Group Range : None
MVR Max Multicast Groups : 128
MVR Current Multicast Groups : 0
MVR Global query response time : 1 sec
MVR Mode : compatible
```

17.3. mvr group

Item	Description
Syntax	mvr group <ip-address> [<1-128>]
Parameter	**< ip-address>:** Start MVR IP multicast address
	[<1-128>]: Contiguous series of IP addresses.
Default	
Mode	Global Configuration
Usage	Use the **mvr group** command to configure mvr group address range when mvr is enabled. The command will delete all mvr vlan ipv4 group entry You can verify settings by the **show mvr** command

Example:

The following example specifies that set mvr group range is 224.1.1.1 ~224.1.1.8 test.

```
Switch(config)# mvr
Switch(config)# mvr group 224.1.1.1 8
The operation will delete the MVR VLAN groups include static MVR
groups.Continue? [yes/no]:y
Switch# show mvr
MVR Running : Enabled
```

```
MVR Multicast VLAN : 2
MVR Group Range : 224.1.1.1 ~ 224.1.1.8
MVR Max Multicast Groups : 128
MVR Current Multicast Groups : 0
MVR Global query response time : 1 sec
MVR Mode : compatible
```

17.4. mvr mode

Item	Description
Syntax	mvr mode (dynamic | compatible)
Parameter	**(dynamic|compatible):** dynamic: Allows dynamic MVR membership on source ports compatible: does not support IGMP dynamic joins on source ports.
Default	Default is compatible.
Mode	Global Configuration
Usage	Use the **mvr mode** command to change mvr mode when mvr is enabled. You can verify settings by the **show mvr** command.

Example:

The following example specifies that set mvr mode dynamic test.

```
Switch(config)# mvr
Switch(config)# mvr mode dynamic
Switch# show mvr
MVR Running : Enabled
MVR Multicast VLAN : 2
MVR Group Range : 224.1.1.1 ~ 224.1.1.8
MVR Max Multicast Groups : 128
MVR Current Multicast Groups : 0
MVR Global query response time : 1 sec
MVR Mode : dynamic
```

17.5. mvr query-time

Item	Description
Syntax	mvr query-time <1-10>
	no mvr query-time
Parameter	**<1-10>**: specifies query response time is 1~10 sec.
Default	Default is 1 sec.
Mode	Global Configuration

Usage	Use the **mvr query-time** command to configure when mvr is enabled. Use the **no** form of this command to set query-time default value. You can verify settings by the **show mvr** command.

Example:

The following example specifies that set mvr query-time 10 sec test.

```
Switch(config)# mvr
Switch(config)# mvr query-time 10
Switch# show mvr
MVR Running : Enabled
MVR Multicast VLAN : 2
MVR Group Range : 224.1.1.1 ~ 224.1.1.8
MVR Max Multicast Groups : 128
MVR Current Multicast Groups : 0
MVR Global query response time : 10 sec
MVR Mode : dynamic
```

17.6. mvr port type

Item	Description
Syntax	mvr type (source | receiver)
	no mvr type
Parameter	**(source | receiver):** Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN. Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages.Receiver ports cannot belong to the multicast VLAN.
Default	
Mode	Port Configuration
Usage	Use the **mvr type** command to configure mvr port type when mvr is enabled. The source port must only belong to mvr vlan. The receiver port must not belong to mvr vlan, and port mode must be access mode. Use the **no** form of this command to set mvr type none You can verify settings by the **show mvr interface** command.

Example:

The following example specifies that set gi1 gi1 is source port , fa2 is receiver port test.

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

```
Switch(config-vlan)# exit
Switch(config)# mvr
Switch(config)# mvr vlan 2
Switch(config)# mvr group 224.1.1.1 8
Switch(config)# interface gi1
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# mvr type source
Switch(config-if)# exit
Switch(config)# interface gi2
Switch(config-if)# switchport mode access
Switch(config-if)# mvr type receiver
Switch# show mvr interface
Port |  Type | Immediate Leave
-----+-------+----------------
gi1 |  Source | Disabled
gi2 | Receiver| Disabled
```

17.7. mvr port immediate

Item	Description
Syntax	mvr immediate no mvr immediate
Parameter	
Default	Default is disabled
Mode	Port Configuration
Usage	Use the **mvr immediate** command to configure mvr support immediate leave when mvr is enabled. Note This command applies to only receiver ports and should only be enabled on receiver ports to which a single receiver device is connected. Use the **no** form of this command to disable immediate leave. You can verify settings by the **show mvr interface** command

Example:

The following example specifies that set gi2 immediate enable test. The configure should configure mvr receiver port firstly.(eg. mvr port type)

```
Switch(config)# interface gi2
Switch(config-if)# mvr immediate
Switch(config-if)# exit
Switch(config)# exit
Switch# show mvr interface
   Port | Type    | Immediate Leave
   -----+---------+----------------
   gi1 |  Source | Disabled
```

```
gi2  | Receiver| Enabled
```

17.8. mvr vlan group

Item	Description
Syntax	mvr vlan <VLAN-ID> group <ip-addr> interfaces IF_PORTS
	no mvr vlan < VLAN-ID> group <ip-addr> interfaces IF_PORTS
Parameter	**VLAN-ID:** specifies MVR VLAN ID for static group
	ip-addr: specifies multicast MVR group address
	IF_PORTS: specifies port list to set or remove
Default	
Mode	Global Configuration
Usage	Use the **mvr vlan group** command to add a static group or configure static group member ports when mvr is enabled. This command applies to only receiver ports. In compatible mode, this command applies to only receiver ports. In dynamic mode, it applies to receiver ports and source ports. When remove static mvr group all ports, the static group will be delete. Or can use **no ip igmp vlan VLAN-ID group** to delete the mvr static group. Static group can't learn dynamic port by igmp memesage. Use the **no** form of this command to delete a port in static group. If remove the last member of static group, the static group will be delete. You can verify settings by the **show mvr members** command.

Example:

The following example specifies that set mvr static group test.The configure must configure mvr receiver port firstly.(eg. mvr port type) Switch(config)# mvr vlan 2 group 224.1.1.1 interfaces gi2

```
Switch# show mvr members
Gourp IP Address | Type | Life(Sec) | Port
----------------+--------+---------+-----------------
       224.1.1.1 | Static|   --    | gi2

  Total Number of Entry = 1
```

17.9. clear mvr members

Item	Description
Syntax	clear mvr members [dynamic|static]
Parameter	dynamic specifies MVR dynamic group
	static specifies MVR static group

Default	Clear all of mvr group
Mode	Privileged EXEC
Usage	This command will clear the mvr groups for selected type.

Example:

The following example specifies that clear all mvr groups test.

```
Switch# clear mvr members
```

17.10. show mvr members

Item	Description
Syntax	show mvr members
Parameter	
Default	
Mode	Privileged EXEC
Usage	This command will display the mvr groups for all of type.

Example:

The following example specifies that show mvr groups test.

```
Switch# show mvr members
```

17.11. show mvr interface

Item	Description
Syntax	show mvr interface [IF_PORTS]
Parameter	IF_PORTS Show specifies port list configurationt
Default	
Mode	Privileged EXEC
Usage	This command will display mvr port type and port immediate status.

Example:

The following example specifies that show mvr interface test.

```
Switch# show mvr interface
```

17.12. show mvr

Item	Description
Syntax	show mvr
Parameter	
Default	
Mode	Privileged EXEC
Usage	This command will display mvr global information.

Example:

The following example specifies that show mvr test.

```
Switch# show mvr
MVR Running : Enabled
MVR Multicast VLAN : 100
MVR Group Range : 224.1.1.1 ~ 224.1.1.128
MVR Max Multicast Groups : 128
MVR Current Multicast Groups : 0
MVR Global query response time : 1 sec
MVR Mode : compatible
```

18. Port

18.1. back-pressure

Item	Description
Syntax	back-pressure no back-pressure
Parameter	
Default	Default back pressure state is enabled.
Mode	Interface Configuration
Usage	Use "**back-pressure**" command to make port to enable back pressure feature. Use **no** form of this command to disable back pressure feature. The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to configure port gi1 and gi2 to be protected port.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# no back-pressure
```

This example shows how to show current back pressure

```
Switch# show running-config interface GigabitEthernet1
interface gi1
    no back-pressure
```

18.2. clear interface

Item	Description
Syntax	clear interfaces IF_PORTS counters
Parameter	IF_PORTS Specify port to clear counters.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**clear interface**" command to clear statistic counters on specific ports.

Example:

This example shows how to clear counters on port gi1.

```
Switch(config)# clear interfaces gi1 counters
```

This example shows how to show current counters

```
Switch# show interfaces gi1
Hardware is Fast Ethernet
Auto-duplex, Auto-speed, media type is Copper flow-control is off
0 packets input, 0 bytes, 0 throttles Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 PAUSE output
```

18.3. description

Item	Description
Syntax	description WORD<1-32>
	no description
Parameter	WORD<1-32> Specifiy port description string.
Default	Default port description is empty.
Mode	Interface Configuration
Usage	Use "**description**" command to give the port a name to identify it easily. If description includes space character, please use double quoted to wrap it. Use **no** form to restore description to empty string.

Example:

This example shows how to modify port descriptions.

```
Switch(config)# interface GigabitEthernet1
Switch(config-if)# description userport
Switch(config-if)#  exit
Switch(config)# interface GigabitEthernet2
Switch(config-if)# description "uplink port"
```

This example shows how to show current port description on interface gi1 and gi2

```
Switch# show interfaces Gi1-2 status
Port  Name               Status      Vlan  Duplex  Speed    Type
gi1   userport           notconnect  1     auto    auto     Copper
gi2   uplink port        notconnect  1     auto    auto     Copper
```

18.4. Duplex

Item	Description
Syntax	duplex (auto | full | half)
Parameter	**auto**: Specify port duplex to auto negotiation.
	full: Specify port duplex to force full duplex.
	half :Specify port duplex to force half duplex.
Default	Default port duplex is auto.
Mode	Interface Configuration
Usage	Use "**duplex**" command to change port duplex configuration.

Example:

This example shows how to modify port duplex configuration.

```
Switch(config)# interface GigabitEthernet1
Switch(config-if)# duplex full
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet2
Switch(config-if)# duplex half
```

This example shows how to show current speed configuration

```
Switch# show running-config interfaces GigabitEthernet1-2
interface gi1
duplex full interface gi2 duplex half
```

This example shows how to show current interface link speed

```
Switch# show interfaces GigabitEthernet1-2 status
Port   Name        Status      Vlan  Duplex  Speed   Type
gi1    userport    notconnect   1    full    auto    Copper
gi2    uplinkport  notconnect   1    half    auto    Copper
```

18.5. eee

Item	Description
Syntax	eee
	no eee
Parameter	
Default	Default eee state is disabled.
Mode	Interface Configuration
Usage	Use "**eee**" command to make port to enable the energy efficient Ethernet feature.Use **no** form of this command to disable eee.The only way to show

	this configuration is using "**show running-config**" command.

Example:

This example shows how to configure port gi1 to enable EEE.

```
Switch(config)# interface Gi1
Switch(config-if)# eee
```

This example shows how to show current EEE

```
Switch# show running-config interface GigabitEthernet1
interface gi1
eee
```

18.6. flowcontrol

Item	Description
Syntax	flowcontrol (auto | off | on)
	no flowcontrol
Parameter	**auto:**Automatically enables or disables flow control on the interface.
	off: Disable port flow control.
	on: Enable port flow control.
Default	Default port flow control is off.
Mode	Interface Configuration
Usage	Use "**flowcontrol**" command to change port flow control configuration. Use **no** form to restore flow control to default (off) configuration.

Example:

This example shows how to modify port duplex configuration.

```
Switch(config)# interface GigabitEthernet1
Switch(config-if)# flowcontrol on
```

This example shows how to show current flow control configuration

```
Switch# show interfaces GigabitEthernet1
Hardware is Fast Ethernet
Full-duplex, Auto-speed, media type is Copper
flow-control is on
0 packets input, 0 bytes, 0 throttles Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
379 packets output, 31981 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
```

```
0 PAUSE output
```

18.7. jumbo-frame

Item	Description
Syntax	jumbo-frame
	no jumbo-frame
Parameter	
Default	Default maximum frame size is disable/1522byte,Enable/12288 byte.
Mode	Global Configuration
Usage	Use "**jumbo-frame**" command to modify maximum frame size to 12288. Use "**no jumbo-frame**" command to modify maximum frame size to 1522. The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to modify maximum frame size on gi1 to 12288 bytes.

```
Switch(config)# jumbo-frame
```

This example shows how to show current jumbo-frmae size

```
Switch# show running-config
jumbo-frame
```

18.8. show interface

Item	Description
Syntax	show interfaces IF_PORTS
	show interfaces IF_PORTS status
	show interfaces IF_PORTS uptime
Parameter	**IF_PORTS:** Specifiy port to show.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show interface**" command to show detail port counters, parameters and status. Use "**show interface status**" command to show brief port status. Use "**show interface uptime**" command to show port uplink time.

Example:

This example shows how to show current counters

```
Switch# show interfaces gi1
```

```
Hardware is Fast Ethernet
Auto-duplex, Auto-speed, media type is Copper flow-control is off
0 packets input, 0 bytes, 0 throttles Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 PAUSE output
```

This example shows how to show current port uplink time.

```
Switch# show interfaces gi1-2 uptime
Port   |               Uptime
-------+-----------------------------------------
gi1    |   0 days, 0 hours, 0 mins, 0 secs
gi2    |   0 days, 0 hours, 0 mins, 0 secs
```

This example shows how to show current port status

```
Switch# show interfaces gi1-2 status

Port  Name          Status      Vlan  Duplex  Speed    Type
gi1                 notconnect   1     auto    auto     Copper
gi2                 notconnect   1     auto    auto     Copper
```

18.9. speedCopperGiga

Item	Description
Syntax	speedCopperGiga (10 | 100 | 1000)
	speedCopperGiga auto [(10 | 100 | 1000 | 2500 | 10/100)]
	speedFiber(1000|10000)
	speed nonegtiate
	no speed nonegotiate
Parameter	**10:** Specify port speed to force 10Mbits/s or auto with 10Mbits/s ability.
	100: Specify port speed to force 100Mbits/s or auto with 100Mbits/s ability.
	1000: Specify port speed to force 1000Mbits/s or auto with 1000Mbits/s ability.
	2500: Specify port speed to auto with 1000Mbits/s ability.
	10/100: Specify port speed to auto with 10Mbits/s and 100Mbits/s.
	10000/1000: Specify Fiber port speed to force 10000Mbits/s or 1000Mbits/s.
Default	Default port speed is auto with all available abilities.
Mode	Interface Configuration

Usage	Use "**speedCopperGiga**" command to change port speed configuration. The speed is only able to configure to the physical maximum speed. For example, in fast Ethernet port, speed 10000 is not available. You cannot configure the speed on the SFP module ports, but you can configure the speed to not negotiate (nonegotiate) if it is connected to a device that does not support autonegotiation.

Example:

This example shows how to modify port speed configuration.

```
Switch(config)# interface GigabitEthernet1
Switch(config-if)#speedCopperGiga 100
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet2
Switch(config-if)#speedCopperGiga auto 1000
Switch(config)#interface XGigabitEthernet 1
Switch(config-if)#no speed nonegotiate
Switch(config)# interface XGigabitEthernet 1
Switch(config-if)#speed nonegotiate
Switch(config)# interface XGigabitEthernet 1
Switch(config-if)# speedFiber 10000
```

This example shows how to show current speed configuration

```
Switch# show running-config interfaces GigabitEthernet1-2
interface gi1
               speedCopperGiga 100
interface gi2
               speedCopperGiga auto 1000
Switch# show running-config interfaces XGigabitEthernet 1
interface xgi1
               speed nonegotiate
               speedFiber 10000
```

This example shows how to show current interface link speed

```
Switch# show interfaces gi1-2 status
Port  Name               Status      Vlan  Duplex  Speed    Type
gi1                     notconnect  1     auto    100M     Copper
gi2                     notconnect  1     auto    auto     Copper

Switch# show interfaces XGigabitEthernet 1 status
Port  Name              Status      Vlan  Duplex  Speed    Type
xgi1                    notconnect   1     full    10G      Fiber
```

18.10. shutdown

Item	Description
Syntax	shutdown
	no shutdown
Parameter	
Default	Default port admin state is no shutdown.
Mode	Interface Configuration
Usage	Use "**shutdown**" command to disable port and use "**no shutdown**" to enable port. If port is error disabled by some reason, use "**no shutdown**" command can also recovery the port manually.

Example:

This example shows how to modify port duplex configuration.

```
Switch(config)# interface Gi1
Switch(config-if)# shutdown
```

This example shows how to show current admin state configuration

```
Switch# show running-config interfaces Gi1
interface gi1
shutdown
```

This example shows how to show current link status

```
Switch# show interfaces gi1 status
Port  Name  Status   Vlan   Duplex   Speed   Type
gi1         disable   1      full      auto   Copper
```

18.11. Traffic Segmentation

Item	Description
Syntax	show traffic_segmentation [PORTLIST]
	traffic_segmentation PORTLIST forward_list [PORTLIST]
Parameter	**PORTLIST:** Port List (e.g. gi2,gi3-8,10gi1-3).Notice: Not included LAG port.
Default	Default port admin state is no shutdown.
Mode	global Configuration
Usage	Use "**traffic_segmentation**" command to configure physical port settings to prevent ports from communicating with each other. One or more ports can be set to forward packets to the specified one or more ports to achieve port isolation in the physical layer.

Example:

This example shows how to set the port isolation configuration.

```
Switch(config)#traffic_segmentation gi1-gi2 forward_list gi3-gi4
Switch# show traffic_segmentation
 Port   | Forward Portlist
--------+-----------------
    gi1 |   gi3-4
    gi2 |   gi3-4
    gi3 |gi1-24,xgi1-4
    gi4 |gi1-24,xgi1-4
    gi5 |gi1-24,xgi1-4
    gi6 |gi1-24,xgi1-4
--More-
```

19. Port Error Disable

19.1. errdisable recovery cause

Item	Description
Syntax	errdisable recovery cause (all|acl|arp-inspection|bpduguard|broadcast-flood|dhcp-rate-limit|psecure-violation|selfloop|unicast-flood|unknown-multicastflood)
	no errdisable recovery cause (all|acl|arp-inspection|bpduguard|broadcast-flood|dhcp-rate-limit|psecure-violation|selfloop|unicast-flood|unknown-multicastflood)
Parameter	**all:** Enable the auto recovery for port error disabled from all causes.
	acl: Enable the auto recovery for port error disabled from the ACL cause.
	arp-inspection: Enable the auto recovery for port error disabled from the ARP inspection cause.
	bpduguard: Enable the auto recovery for port error disabled from the STP BPDU Guard cause**.**
	broadcast-flood: Enable the auto recovery for port error disabled from the broadcast flooging cause.
	dhcp-rate-limit: Enable the auto recovery for port error disabled from the DHCP rate limit cause.
	psecure-violation: Enable the auto recovery for port error disabled from the port security cause.
	selfloop: Enable the auto recovery for port error disabled from the STP self-loop cause.
	unicast-flood: Enable the auto recovery for port error disabled from the unicast flooding cause.
	unknown- multicastflood: Enable the auto recovery for port error disabled from the unknown multicast flooding cause.
Default	Error disable recovery is disabled for all cause.
Mode	Global Configuration
Usage	Ports would be disabled because of the invalid actions detected by protocols. To enable the port error disable recovery from the specific cause, use the command **errdisable recovery cause** in the Global Configuration mode.

Example:

The following example enables the port error disable recovery for the STP BPDU Guard and self-loog cause.

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)# errdisable recovery cause selfloop
```

19.2. errdisable recovery interval

Item	Description
Syntax	errdisable recovery interval seconds
Parameter	**seconds:** The time in seconds to recover from a specific error-disable state. The vaild range is 0 to 86400 seconds,and the default value is 300 seconds.
Default	The default recovery time is 300 seconds.
Mode	global Configuration
Usage	To set the recovery time of the error disabled ports, use the command **errdisable recovert interval** in the Global Configuration mode.

Example:

The following example set the agimg time to 500 seconds.

```
Switch(config)# errdisable recovery interval 60
```

19.3. show errdisable recovery

Item	Description
Syntax	show errdisable recovery
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the error disable configuration and the interfaces in the error disabled state, use the command **show errdisable recovery** in the Privileged EXEC mode.

Example:

The following example shows the error disable configuration, and the interfaces in the error disabled state.

```
Switch# show errdisable recovery
ErrDisable Reason   | Timer Status
--------------------+--------------
Bpduguard           | enabled
Selfloop            | enabled
broadcast-flood     | disabled
unknown-multicast-flood | disabled
unicast-flood       | disabled
acl                 | disabled
psecure-violation   | disabled
```

```
dhcp-rate-limit    | disabled
arp-inspection     | disabled

Timer Interval : 60 seconds
Interfaces that will be enabled at the next timeout:
Port |  Error Disable Reason   | Time Left
-----+-------------------------+------------
```

20. Port Security

20.1. port-security (Global)

Item	Description
Syntax	port-security no port-security
Parameter	
Default	Default is disabled
Mode	Global Configuration
Usage	The "**port-security**" command enables the port security functionality globally.Use the **no** form of this command to disable. You can verify settings by the **show port-security** command.

Example:

The following example shows how to enable port security

```
switch(config)# port-security
switch# show port-security
port-security is:  Enabled
```

20.2. port-security (Interface)

Item	Description
Syntax	port-security no port-security
Parameter	
Default	Default is disabled
Mode	Port Configuration
Usage	The "**port-security**" command enables the port security functionality on this port.Use the **no** form of this command to disable You can verify settings by the **show port-security** interface command.

Example:

The following example shows how to enable port security on interface GigabitEthernet1

```
switch(config)# interface gi1
switch(config-if)# port-security
switch(config)# show port-security interfaces gi1
Port    |   Security    | CurrentAddr |Action
--------+-------------+--------------+---------------------
gi1  |  Enabled (  1)  |    0   |   Discard
```

20.3. port-security address-limit

Item	Description
Syntax	port-security address-limit <1-256> action (forward|discard|shutdown)
	no port-security address-limit
Parameter	**<1-256>:**The learning-limit number. It specifies how many MAC addresses this port can learn.
	forward: Forward this packet whose SMAC is new to system and exceed the learning-limit number.
	discard:Discard this packet whose SMAC is new to system and exceed the learning-limit number.
	shutdown: Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.
Default	The address-limit default is 1 and action is “drop”.
Mode	Port Configuration
Usage	Use the “**port-security address-limit**” command to set the learning-limit number and the violation action. Use the **no** form of this command to restore the default settings. You can verify settings by the **show port-security interface** command.

Example:

The following example shows how to enable port security on port 1 and set the learning limit number to 10.

```
switch(config)# interface gi1
switch(config-if)# port-security address-limit 10 action discard
switch(config-if)# port-security
switch# show port-security interfaces gi1
Port    |  Mode  |  Security    | CurrentAddr |Action
-------+--------+-------------+-------------+-------
  gi1  | Dynamic |  Enabled (  10)  |  0   |   Discard
```

20.4. show port-security

Item	Description
Syntax	show port-security
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use “**show port-security**” command to show port-security global information.

Example:

This example shows how to show port-security configurations.

```
Switch# show port-security
port-security is:  Enabled
```

20.5. show port-security interface

Item	Description
Syntax	show port-security interface IF_PORTS
Parameter	**IF_PORTS:** Select port to show port-security configurations.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show port-security interfaces**" command to show port-security information of the specified port.

Example:

This example shows how to show port-security configurations on interface gi1.

```
Switch# show port-security interfaces gi1
Port    |   Security    | CurrentAddr |Action
--------+-------------+-------------+-------------
gi1   |  Enabled (  10)  | 0   |   Discard
```

21. QoS

21.1. qos

Item	Description
Syntax	qos
	no qos
Parameter	
Default	Default qos is disabled.
Mode	Global Configuration
Usage	Use "**qos**" command to enable quality of service which according to basic trust type to assign queue for packets, and packets with higher priority are able to send first. Use **no** form of this command to disable quality of service.

Example:

This example shows how to change qos to basic mode.

```
Switch(config)# qos
```

This example shows how to check current qos mode.

```
Switch# show qos
QoS Mode: basic
Basic trust: cos
```

21.2. qos cos

Item	Description
Syntax	qos cos <0-7>
Parameter	**cos <0-7>:** Specify the CoS value for the interface.
Default	Default CoS value for interface is 0.
Mode	Interface Configuration
Usage	Sometimes, there is no qos information in the packets, such as CoS, DSCP, IP Precedence. But we still can give the priority for packets by configuring the interface default cos value. If there is no qos information in the packets, the device will use this default cos value and find the cos-queue map to get the final destination queue. Use "**qos cos**" command to assign port default cos value.

Example:

This example shows how to configure default cos value 7 on interface gi1.

```
Switch(config)# interface gi1
```

```
Switch(config-if)# qos cos 7
Switch(config-if)# end
Switch# show qos interface gi1
Port | CoS  | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
-----+-----+-------------+------------+-------------+--------------
gi1 |   7   |   enabled    |   disabled |   disabled   | disabled |
```

21.3. qos map

Item	Description
Syntax	qos map (cos-queue | dscp-queue | precedence-queue) SEQUENCE to <1- 8>
	qos map (queue-cos | queue-precedence) SEQUENCE to <0-7>
	qos map queue-dscp SEQUENCE to <0-63>
Parameter	**cos-queue**: Configure or show CoS to queue map
	dscp-queue: Configure or show DSCP to queue map
	precedence-queue: Configure or show IP Precedence to queue map.
	queue-cos: Configure or show queue to CoS map
	queue-dscp: Configure or show queue to DSCP map
	queue-precedence: Configure or show queue to IP Precedence map
	SEQUENCE: Specify the cos, dscp, precedence or queue with one or multiple values.
	<1- 8>: Specify th queue id
	<0-7>: Specify the cos or precedence values
	<0-63>: Specify the dscp values
Default	The default values of cos-queue are showing in the following table. cos-queue:0-2,1-1,2-3,3-4,4-5,5-6,6-7,7-8
	The default values of dscp-queue are showing in the following table. dscp-queue:0~7-1,8~15-2,16~23-3,24~31-4,32~39-5,40~47-6,48~55-7,56~64-8
	The default values of ip precedence are showing in the following table. IP precedence-queue:0-1,1-2,2-3,3-4,4-5,5-6,6-7,7-8
	The default values of queue-cos are showing in the following table. queue-cos:1-1,2-0,3-2,4-3,5-4,6-5,7-6,8-7
	The default values of queue-dscp are showing in the following table. queue-dscp:1-0,2-8,3-16,4-24,5-32,6-40,7-48,8-56
	The default values of queue-precedence are showing in the following table queue-precedence:1-0,2-1,3-2,4-3,5-4,6-5,7-6,8-7
Mode	Global Configuration
Usage	According to different trust type, packets will be assigned to different queue based on the specific qos map. For example, if the trust type is trust cos, the device will get the cos value in packet and reference the cos-queue mapping to assign the correct queue. The queue to cos, dscp or precedence maps are used by remarking function. If

	the port remarking feature is enabled, the remarking function will reference these 3 tables to remark packets.

Example:

This example shows how to map cos 6 and 7 to queue 1.

```
Switch(config)# qos map cos-queue 6 7 to 1
Switch# show qos map cos-queue
CoS to Queue mappings
COS 0   1   2   3   4   5   6   7
--------------------------------
Queue   2   1   3   4   5   6   1   1
```

This example shows how to map queue 4 and 5 to cos 7.

```
Switch(config)# qos map queue-cos 4 5 to 7
Switch# show qos map queue-cos
 Queue to CoS mappings
Queue   1   2   3   4   5   6   7   8
-----------------------------------
CoS     1   0   2   7   7   5   6   7
```

21.4. qos queue

Item	Description
Syntax	qos queue strict-priority-num <0-8>
	qos queue weight SEQUENCE
	show qos queueing
Parameter	**strict-priority- num <0-8>:** Specify the strict priority queue number.
	weight SEQUENCE: Specify the non-strict priority queue weight value. The valid queue weight value is from 1 to 127.
Default	Default strict priority queue number is 8, it means all queues are strict priority queue. The default queue weight for each queue is shown in following table. queueID-queue weight:1-1,2-2,3-3,4-4,5-5,6-9,7-13,8-15
Mode	Global Configuration
Usage	The device support total 8 queues for QoS queueing. It is able to set the queue to be strict priority queue or weighted queue to prevent starvation. The queue with higher id value has higher priority. First, you need to decide how many strict priority queue you need. The strict priority queue will always occupy the higher priority queue. For example, if you specify the strict priority number to be 2, then the queue 7 and 8 will be the strict priority queues and the others are weighted queues. After you setup the number of strict priority queue, you need to setup the

	weight for the weighted queues by using “qos queue weight” command. And the bandwidth will shared by the weight you configured between these weighted queues.

Example:

This example shows how to setup device with 3 strict priority queues and give other weighted queues with weight 5, 10, 15, 20, 25.

```
Switch(config)# qos queue strict-priority-num 3
Switch(config)# qos queue weight 5 10 15 20 25
Switch# show qos queueing
qid-weights Ef - Priority
1-  5   dis- N/A
2-  10  dis- N/A
3-  15  dis- N/A
4-  20  dis- N/A
5-  25  dis- N/A
6- N/A  ena- 6
7- N/A  ena- 7
8- N/A  ena- 8
```

21.5. qos remark

Item	Description
Syntax	qos remark (cos | dscp | precedence)
	no qos remark (cos | dscp | precedence)
	show qos queueing
Parameter	**cos:** Enable/Disable cos remarking.
	dscp: Enable/Disable dscp remarking.
	precedence: Enable/Disable precedence remarking.
Default	Default CoS remarking is disabled. Default DSCP remarking is disabled. Default IP Precedence remarking is disabled.
Mode	Interface Configuration
Usage	QoS remarking feature allow you to change priority information in packets based on egress queue. For example, you want all packets egress from interface gi1 queue 1 to remark the cos value to be 5 for next tier of device, you can enable the cos remarking feature on gi1 and configure the queue-cos map for queue 1 map to cos 5. Use “**qos remark**” command to enable remarking feature on specific type. And use “**no qow remark**” command to disable it.

Example:

This example shows how to enable remarking features on interface gi1.

```
Switch(config)# interface Gi1
Switch(config-if)# qos remark cos
Switch(config-if)# qos remark dscp
Switch(config-if)# qos remark precedence
Switch(config-if)# end
Switch# show qos interface Gi1
Port | CoS  | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
-----+-----+-------------+------------+-------------+---------------
  gi1 |  0  |  enabled    |   enabled  |   enabled   |   enabled |
```

21.6. qos trust

Item	Description
Syntax	qos trust (cos | cos-dscp | dscp | precedence)
	no qos trust
Parameter	**cos**: Specify the device to trust CoS
	cos-dscp: Specify the device to trust DSCP for IP packets, and trust CoS for non-IP packets.
	dscp: Specify the device to trust DSCP.
	precedence: Specify the device to trust IP Precedence.
Default	Default QoS trust type is cos.
Mode	Global Configuration
Usage	In QoS basic mode, there are 4 trust types for device to judge the appropriate queue of the packets. This command is able to switch between these trust types. **CoS**: IEEE 802.1p defined 3bits priority value in vlan tag. Trust this value in packets and assign queue according to cos-queue map. **DSCP**: IETF RFC2474 defined 6bits priority value in IP packet (highest 6bits in ToS field). Trust this value in packets and assign queue according to dscp-queue map. **IP Precedence**: The highest 3bits priority value in IP packet ToS field. Trust this value in packets and assign queue according to precedence-queue map. **CoS-DSCP**: Trust DSCP for IP packets and assign queue according to dscp-queue map. Trust CoS for non-IP packets and assign queue according to cos-queue map.

Example:

This example shows how to change qos basic mode trust types.

```
Switch(config)# qos trust cos
Switch(config)# qos trust cos-dscp
```

```
Switch(config)# qos trust dscp
Switch(config)# qos trust precedence
```

This example shows how to check current qos trust type.

```
Switch# show qos
QoS Mode: basic
 Basic trust: ip-precedence
```

21.7. qos trust (Interface)

Item	Description
Syntax	qos trust
	no qos trust
Parameter	
Default	Default interface qos trust state is enabled.
Mode	Interface Configuration
Usage	After QoS function is enabled in basic mode, the device also support per interface enable/disable the qos function. If the trust state on interface is enabled, all ingress packets of this interface will remap according to the trust type and the qos maps. Otherwise, all ingress packets will assign to queue 1. Use "**qos trust**" to enable trust state on interface and use "**no qos trust**" to disable trust state on interface.

Example:

This example shows how to disable qos trust state on interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# no qos trust
Switch(config-if)# end
Switch# show qos interface gi1
Port | CoS  | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
-----+-----+-------------+------------+-------------+---------------
  gi1| 0   |   disabled  |   disabled |   disabled  |  disabled   |
```

21.8. show qos

Item	Description
Syntax	show qos
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC

Usage	Use "**show qos**" command to show qos state and trust type.

Example:

This example shows how to check current qos mode.

```
Switch# show qos
QoS Mode: basic
 Basic trust: cos
```

21.9. show qos interface

Item	Description
Syntax	show qos interface IF_PORTS
Parameter	**IF_PORTS:** Select port to show qos configurations.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show qos interfaces**" command to show port default cos ,remarking state and remarking type state informations.

Example:

This example shows how to show qos configurations on interface gi1.

```
Switch# show qos interface gi1
Port | CoS  | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
-----+------+-------------+------------+-------------+--------------
gi1 |   7   |    enabled   |   disabled  |  disabled   |  disabled  |
```

21.10. show qos map

Item	Description
Syntax	show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos | queue-dscp | queue-precedence)]
Parameter	**cos-queue**:Show CoS to queue map.
	dscp-queue: Show DSCP to queue map.
	precedence-queue:Show IP Precedence to queue map.
	queue-cos:Show queue to CoS map.
	queue-dscp:Show queue to DSCP map.
	queue-precedence:Show queue to IP Precedence map.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show qos map**" command to show all kinds of mapping for qos remapping and remarking features.

Example:

This example shows how to show all qos maps.

```
Switch(config)# show qos map
CoS to Queue mappings
   COS   0  1  2  3  4  5  6  7
--------------------------------
 Queue   2  1  3  4  5  6  1  1

DSCP to Queue mappings
d1: d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0:     1  1  1  1  1  1  1  1  2  2
 1:     2  2  2  2  2  2  3  3  3  3
 2:     3  3  3  3  4  4  4  4  4  4
 3:     4  4  5  5  5  5  5  5  5  5
 4:     6  6  6  6  6  6  6  6  7  7
 5:     7  7  7  7  7  7  8  8  8  8
 6:     8  8  8  8

IP Precedence to Queue mappings
 IP Precedence   0  1  2  3  4  5  6  7
----------------------------------------
        Queue   1  2  3  4  5  6  7  8

Queue to CoS mappings
 Queue   1  2  3  4  5  6  7  8
--------------------------------
   CoS   1  0  2  7  7  5  6  7

Queue to DSCP mappings
 Queue   1  2  3  4  5  6  7  8
--------------------------------
  DSCP   0  8 16 24 32 40 48 56

Queue to IP Precedence mappings
 Queue   1  2  3  4  5  6  7  8
--------------------------------
ipprec   0  1  2  3  4  5  6  7
```

21.11. show qos queueing

Item	Description
Syntax	show qos queueing
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show qos queueing**" command to show qos queueing information.

Example:

This example shows how to check current qos queueing information.

```
Switch# show qos queueing
qid-weights Ef - Priority
1-  3   dis- N/A
2-  5   dis- N/A
3- N/A  ena- 3
4- N/A  ena- 4
5- N/A  ena- 5
6- N/A  ena- 6
7- N/A  ena- 7
8- N/A  ena- 8
```

22. Rate Limit

22.1. rate limit egress

Item	Description
Syntax	rate-limit egress <16-1000000>
	no rate-limit egress
Parameter	**<16-1000000>:** Specify the committed information rate.
Default	Default rate limit is disabled.
Mode	Interface configuration
Usage	Use the "**rate-limit egress**" command to configure the egress port shaper. Use the **no** form of this command to disable the shaper. You can verify your setting by entering the show **running-config interfaces** command.

Example:

The following example show how to configure ingress port rate limit and egress port shaper.

```
Switch(config)# interfaces gi1
Switch(config-if)# rate-limit egress 2048
Switch# show running-config interfaces gi1 interface gi1
    rate-limit egress 2048
```

22.2. rate limit ingress

Item	Description
Syntax	rate-limit ingress <16-1000000>
	no rate-limit ingress
Parameter	**<16-1000000>:** Specify the ingress limit rate
	<1-8>: Specify the egress shaper queue number
Default	Rate limiting is disabled.
Mode	Interface configuration
Usage	Use the "**rate-limit ingress**" command to limit the incoming traffic rate on a port.Use the **no** form of this command to disable the rate limit. You can verify your setting by entering the **show running-config interfaces** command

Example:

The following example show how to configure ingress port rate limit.

```
Switch(config)# interfaces gi1
```

```
Switch(config-if)# rate-limit ingress 128
Switch# show running-config interfaces gi1 interface gi1
rate-limit ingress 128
```

22.3. rate-limit egress queue

Item	Description
Syntax	rate-limit egress queue <1-8> <16-10000000>
	no rate-limit egress queue <1-8>
Parameter	**<16-1000000>:** Specify the committed information rate.
	<1-8>:queue id
Default	Default rate limit is disabled.
Mode	Interface configuration
Usage	Use the "**rate-limit egress queue**" command to configure the queue control rate. Use the **no** form of this command to restore to default setting.

Example:

The following example show how to configure queue control rate.

```
Switch(config-if)# rate-limit egress queue 1 32
```

23. SNMP

23.1. show snmp

Item	Description
Syntax	show snmp
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the status of Simple Network Management Protocol (SNMP), use the command **show snmp** in the Privileged EXEC mode.

Example:

The following example shows the SNMP status.

```
Switch# show snmp
 SNMP is disabled.
```

23.2. show snmp community

Item	Description
Syntax	show snmp community
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the configuration of snmp communities, use the command **show snmp community** in the Privileged EXEC mode.

Example:

The following example shows the SNMP communities configuration.

```
Switch# show snmp community
Commnunity Name      Group Name                    View       Access
---------------- ------------------------ ------------ ---------
  public                                      all           rw

Total Entries: 1
```

23.3. show snmp engineid

Item	Description
Syntax	show snmp engineid
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the SNMPv3 engine IDs defined on the switch, use the command **show snmp engineid** in the Privileged EXEC mode.

Example:

The following example shows the SNMP engind id information.

```
Switch# show snmp engineid
Local SNMPV3 Engine id: 80006a920300e04c000000

    IP address                 Remote SNMP engineID
---------------------------- ----------------------------------

Total Entries: 0
```

23.4. show snmp group

Item	Description
Syntax	show snmp engineid
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the SNMP group configuration on the switch, use the command **show snmp group** in the Privileged EXEC mode.

Example:

The following example shows the SNMP group configuration.

```
Switch# show snmp group
Group Name  Model  Level  ReadView  WriteView  NotifyView
---------- ------ ------- --------- ---------- -----------

 Total Entries: 2
```

23.5. show snmp host

Item	Description
Syntax	show snmp host
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the SNMP trap notification recipients defined on the switch, use the command **show snmp host** in the Privileged EXEC mode.

Example:

The following example shows the configuration of SNMP notification recipients on the switch.

```
Switch# show snmp host
Server   Community Name   Notification  Version  Notification  Type
------  ---------------  ------------  -------  ------------ ---------

 Total Entries: 1
```

23.6. show snmp trap

Item	Description
Syntax	show snmp trap
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the status of SNMP traps on the switch, use the command **show snmp trap** in the Privileged EXEC mode.

Example:

The following example shows the status of SNMP traps.

```
Switch# show snmp trap
SNMP auth failed trap  : Enable
SNMP linkUpDown trap   : Enable
SNMP cold-start trap   : Enable
SNMP warm-start trap   : Enable
SNMP newRoot trap   : Enable
SNMP togogyChgEnable trap   : Enable
```

23.7. show snmp view

Item	Description
Syntax	show snmp view
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the SNMP view defined on the switch, use the command **show snmp view** in the Privileged EXEC mode.

Example:

The following example shows the configuration of SNMP view.

```
Switch# show snmp view
View Name     Subtree OID     OID Mask     View Type
---------- --------------    ----------  --------------------------
all            .1              all        included

Total Entries: 1
```

23.8. show snmp user

Item	Description
Syntax	show snmp user
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the SNMP users defined on the switch, use the command **show snmp user** in the Privileged EXEC mode.

Example:

The following example shows the configuration of SNMP user.

```
Switch# show snmp user Username:  v3
Password:  ********
Privilege Mode:          rw
Access GroupName:        v3
Authentication Protocol: md5
Encryption Protocol:     none
Access SecLevel:         auth
```

```
Total Entries: 1
```

23.9. snmp

Item	Description
Syntax	snmp
	no snmp
Parameter	
Default	SNMP is disabled by default
Mode	Global Configuration
Usage	To enable the SNMP on the switch, use the command **snmp** in the Global Configuration mode. Otherwise, use the **no** form of the command to disable to SNMP

Example:

The following example enables the SNMP.

```
Switch(config)# snmp
```

23.10. snmp community

Item	Description
Syntax	snmp community community-name [view view-name] (ro|rw)
	snmp community community-name group group-name
	no snmp community community-name
Parameter	**community-name**: The SNMP community name. Its maximum length is 20 characters.
	view view-name: Specify the SNMP view configured by the command snmp view to define the object available to the community.
	ro: Read only access (default)
	rw: Writable access
	group group-name: Specify the SNMP group configured by the command snmp group to define the object available to the community.
Default	No SNMP community is configured
Mode	Global Configuration
Usage	To define the SNMP community that permit access for SNMP v1 and v2, use the command **snmp community** in the Global Configuration mode.

Example:

The following example defines the SNMP community named private with the default view all, and the access right is read-only.

```
Switch(config)# snmp community private ro
```

23.11. snmp engineid

Item	Description
Syntax	snmp engineid (default|ENGINEID)
Parameter	**default**: Default engine ID generated on the basis of the switch MAC address.
	ENGINEID: Specify SNMP engine ID. The engine ID is the 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
Default	The default SNMP engine ID on the switch is based on switch MAC address.
Mode	Global Configuration
Usage	To define the SNMP engine on the switch, use the command **snmp engineid** in the Global Configuration mode.

Example:

The following example configure the switch SNMP engine ID

```
Switch(config)# snmp engineid 00036D001122
```

23.12. snmp engineid rmote

Item	Description
Syntax	snmp engineid remote (ip-addr|ipv6-addr) ENGINEID
	no snmp engineid remote (ip-addr|ipv6-addr)
Parameter	**ENGINEID:** Specify SNMP engine ID. The engine ID is a 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
	ip-addr: IP address of the remote host.
	ipv6-addr: IPv6 address of the remote host.
Default	
Mode	Global Configuration
Usage	To define the remote host for SNMP engine, use the command **snmp engineid** remote in the Global Configuration mode; and use the no form of the command to delete the remote host from the SNMP engine.

Example:

The following example adds the remote 192.168.1.11 into SNMP engine

```
Switch(config)# snmp engineid remote 192.168.1.11 00036D10000A
```

23.13. snmp group

Item	Description
Syntax	snmp group group-name (1|2c|3) (noauth|auth|priv) read-view read-view write-view write-view [notify-view notify-view]
	no snmp group group-name security-mode version (1|2c|3)
Parameter	**group-name:** Specify SNMP group name, and the maximum length is 30 characters.
	(1|2c|3): Specify the SNMP version.
	noauth: Specify that no packet authentication is performed.
	auth: Specify that no packet authentication without entryption is performed. It is applicable only to the SNMPv3 security mode.
	priv: Specify that no packet authentication with entryption is performed. It is applicable only to the SNMPv3 security mode.
	read-view read- view: Set the view name that enables configuring the agent and its maximum length is 30 characters.
	write-view write- view: Set the view name that enables viewing only, and its maximum length is 30 characters.
	notify-view notify- view: Sets the view name that sends only traps with contents that is included in SNMP view selected for notification.The maximum length is 30 characters.
Default	No group entry is existed.
Mode	Global Configuration
Usage	To define the SNMP group, use the command **snmp group** in the Glocal Configuration mode, and use the **no** form of the command to delete the configuration. SNMP group configuration is used in the command **snmp use** to map SNMP users to the SNMP group. These users would be automatically maped to the SNMP views defined in this command. The securety level for SNMP v1 or v2 is always **noauth**.

Example:

The following example adds SNMPv3 group

```
Switch(config)# snmp group v3 version 3 auth read-view all write-view all
notify-view all
```

23.14. snmp host

Item	Description
Syntax	snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c)] community-name [udp-port udp-port] [timeout timeout] [retries retries]

	snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] version 3 [(auth|noauth|priv)] community-name [udp-port udp-port] [timeout timeout] [retries retries]
	no snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c|3)]
Parameter	**ip-addr:** The IP adderss of recipet.
	ipv6-addr: The IPv6 adderss of recipet.
	hostname: The host name of recipet.
	traps: Send SNMP traps to the host. It is the default action.
	informs: Send SNMP informs to the host.
	version (1|2c|3): Specify the SNMP version.
	noauth: Specify that no packet authentication is performed. It is applicable only to the SNMPv3 security mode.
	auth: Specify that no packet authentication without entryption is performed. It is applicable only to the SNMPv3 security mode.
	priv: Specify that no packet authentication with entryption is performed. It is applicable only to the SNMPv3 security mode.
	community-name: The SNMP community sent with the notification.
	udp-port udp-port: Specify the UDP port number.
	timeout timeout: Specify the SNMP informs timeout
	retries retries: Specify the retry counter of the SNMP informs.
Default	No SNMP host is configured. The default SNMP version for the command is SNMPv1.
Mode	Global Configuration
Usage	To configure the hosts to receive SNMP notificatons, use the command **snmp host** in the Global Configuration mode; and use the **no** form of the command to delete the configuration.

Example:

The following example adds the recipet 192.168.1.11 for the SNMP traps notification.

```
Switch(config)# snmp host 192.168.1.11 private
```

23.15. snmp trap

Item	Description
Syntax	snmp trap (auth|cold-start|linkUpDown|port-security|warm-start)
	no snmp trap (auth|cold-start|linkUpDown|port-security|warm-start)
Parameter	**auth**: Enable the SNMP authentication failure trap.
	cold-start: Enable the SNMP cold start-up failure trap.
	linkUpDown: Enable the SNMP link up and down failure trap.
	port-security: Enable the SNMP port security trap.
	warm-start: Enable the SNMP warm start-up failure trap.
Default	All the SNMP traps are enabled.

Mode	Global Configuration
Usage	To send the **SNMP traps**, use the command snmp trap in the Global Configuration mode; and use the **no** form of the command to disable the SNMP traps.

Example:

The following example disables and enables the SNMP link up and down traps individually.

```
Switch(config)# no snmp trap linkUpDown
Switch(config)# snmp trap linkUpDown
```

23.16. snmp user

Item	Description
Syntax	snmp user username group-name [auth (md5|sha) AUTHPASSWD]
	snmp user username group-name auth (md5|sha) AUTHPASSWD priv PRIVPASSWD
	no snmp user username
Parameter	**username**: Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the user name must match the community name by the command snmp host.
	group-name: Specify the SNMP group to which the SNMP user belongs.The SNMP group should be SNMPv3 and configured by the command snmp group.
	auth (md5|): Specify the HMAC-MD5-96 authentication protocol as the user authentication.
	auth (sha|): Specify the HMAC-SHA-96 authentication protocol as the user authentication.
	AUTHPASSWD: The password for authentication and the range of length is from 8 to 32 characters.
	Priv PRIVPASSWD: The private password for the privacy key, and the range of length is from 8 to 64 characters.
Default	
Mode	Global Configuration
Usage	To define a SNMP user, use the command snmp user in the Global Configuration mode; and use the no form to delete the SNMP user.

Example:

The following example adds SNMP user v3 into the group v3 by the MD5 authentication.

```
Switch(config)# snmp user v3 v3 auth md5 12345678
```

23.17. snmp view

Item	Description
Syntax	snmp view view-name subtree oid-tree oid-mask (all|oid-mask) viewtype (included|excluded)
	no snmp view view-name subtree (all|oid-tree)
Parameter	**view-name**: The SNMP view name. Its maximum length is 30 characters.
	subtree oid-tree: Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view.
	oid-mask (all|oid- mask): Specify the OID family mask. It is used to define a family of view subtrees. For example, OID mask FA.80 is 11111010.10000000. The length of the OID mask must be less than the length of subtree OID.
	viewtype(included|excluded): Include or exclude the selected MIBs in the view
Default	
Mode	Global Configuration
Usage	To configure the SNMP view, use the command **snmp view** in the Global Configuration mode; and use the **no** form of the command to delete the SNMP view. The default SNMP view cannot be deleted and modified by users. By default, the maximum numbers of SNMP view is limited to 16.

Example:

The following example defines the SNMP view.

```
Switch(config)# snmp view private subtree 1.3.3.1 oid-mask all viewtype
included
```

24. Spanning Tree

24.1. instance (MST)

Item	Description
Syntax	instance instance-id vlan vlan-list
	no instance instance-id vlan vlan-list
Parameter	**instance-id**: The MSTP instance ID from 0 to 15.
	vlan vlan-list: Add the VLAN list to the MSTP instance.
Default	All VLANs are mapped to the Common and Internal Spanning Tree (CIST) instance (instance 0).
Mode	MST Configuration
Usage	To map the VLAN to the Multiple Spanning Tree (MSTP) instances, use the command instance in the MST Configuration mode and use the no form of the command to restore its default configuration. All VLANs that are not explicility configured to an MSTP instance are mapped to the CIST instance (instance 0). For two or more switches in the samp MSTP regiom, their VLAN mapping, name and revision number configuration, must be the same.

Example:

The following example maps the vlan 10-20 to the MSTP instance 1, and VLAN 100 to instance 2.

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# instance 2 vlan 100
```

24.2. name (MST)

Item	Description
Syntax	name name-str
	no name
Parameter	**name-str:** The MSTP instance name. Its maximum length is 32 characters.
Default	The default MSTP name is the switch MAC address.
Mode	MST Configuration
Usage	To define the name for MSTP instance, use the command **name** in the MST Configuration mode; and use the **no** form to restore the default name configuration.

Example:

The following example configures the name of MST instance to Valkyrie.

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name Valkyrie
```

24.3. revision (MST)

Item	Description
Syntax	revision rev
	no revision
Parameter	**rev**: The MSTP revision number. Its valid rage is from 0 to 65535.
Default	The default revision number is 0.
Mode	MST Configuration
Usage	To define the revision for the MSTP configuration, use the command **revision** in the MST Configuration mode; and use the **no** form of the command to restore it default configuration.

Example:

The following example defines the revision MSTP configuration to 1.

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 1
```

24.4. show spanning-tree

Item	Description
Syntax	show spanning-tree
Parameter	
Default	
Mode	Privileged EXEC
Usage	To display the spanning tree configuration, use the command spanning-tree in the Privileged EXEC mode

Example:

The following example shows the spanning tree configuration.

```
Switch# show spanning-tree


Spanning tree enabled mode RSTP
Default port cost method:  long

Root ID    Priority    32768
```

```
Address     00:e0:4c:00:00:00
This switch is the root
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Number of topology changes 1 last change occurred 00:00:08 ago
Times:  hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15

Interfaces
  Name     State   Prio.Nbr   Cost    Sts   Role EdgePort      Type
--------- -------- -------- -------- ---- ---- ----------- ------------
  gi24     enabled  128.24   20000   Frw   Desg   No       P2P (RSTP)
```

24.5. show spanning-tree interface

Item	Description
Syntax	show spanning-tree interface IF_PORTS [statistic]
Parameter	**Interface IF_PORTS**:An interface ID or the list of interface IDs.
	statistic: Display the STP statistic for an interface.
Default	
Mode	Privileged EXEC
Usage	To show the STP configuration and statistics for an interface, use the command **show spanning-tree interface** in the Privileged EXEC mode.

Example:

The following example shows the STP configuration for the interface gi24.

```
Switch# show spanning-tree interfaces gi24
Port gi24 enabled
State: forwarding                          Role: designated
Port id: 128.24                            Port cost: 20000
Type: P2P (RSTP)                           Edge Port: No
Designated bridge Priority : 32768        Address: 00:e0:4c:00:00:00
Designated port id: 128.24                 Designated path cost: 0
BPDU Filter: Disabled                       BPDU guard: Disabled
BPDU: sent 93, received 0
```

The following example shows the STP statistic for the interface gi24.

```
Switch# show spanning-tree interfaces gi24 statistic
STP Port Statistics
==================================================

Port                          : gi24
```

```
Configuration BDPUs Received    : 0
TCN BDPUs Received              : 0
MSTP BDPUs Received             : 0
Configuration BDPUs Transmitted : 0
TCN BDPUs Transmitted           : 0
MSTP BDPUs Transmitted          : 114
================================================
```

24.6. show spanning-tree mst

Item	Description
Syntax	show spanning-tree mst instace-id
Parameter	**instance-id:** The MSTP instance ID. Its valid range is from 0 to 15.
Default	
Mode	Privileged EXEC
Usage	To show the information for a specific MSTP instance, use the command **show spanning-tree mst** in the Privileged EXEC mode.

Example:

The following example displays the information for the MSTP instance 0 and 1 individually.

```
Switch# show spanning-tree mst 0
            MST Instance Information
============================================================
                  Instance Type : CIST (0)
               Bridge Identifier : 32768/ 0/00:E0:4C:00:00:00
------------------------------------------------------------
            Designated Root Bridge : 32768/ 0/00:E0:4C:00:00:00
            External Root Path Cost : 0
                Regional Root Bridge : 32768/ 0/00:E0:4C:00:00:00
            Internal Root Path Cost : 0
                Designated Bridge : 32768/ 0/00:E0:4C:00:00:00
                       Root Port : 0/0
                           Max Age : 20
                   Forward Delay : 15
                   Topology changes : 1
               Last Topology Change : 582
------------------------------------------------------------
            VLANs mapped: 1-9,21-99,101-4094
============================================================

Interface       Role  Sts    Cost      Prio.Nbr Type
```

```
------------ ------- ---- --------- -------- ---------------
gi24            Desg   FWD    20000     128.24   P2P (RSTP)

Switch# show spanning-tree mst 1
MST Instance Information
============================================================
           Instance Type : MSTI (1)
       Bridge Identifier : 32768/ 0/00:E0:4C:00:00:00
------------------------------------------------------------
    Regional Root Bridge : 32768/ 0/00:E0:4C:00:00:00
  Internal Root Path Cost : 0
          Remaining Hops : 20
        Topology changes : 1
    Last Topology Change : 728
------------------------------------------------------------
 VLANs mapped: 10-20
============================================================

Interface       Role  Sts    Cost      Prio.Nbr Type
------------ ------ ----- --------- -------- -------------------
gi24            Desg    FWD    20000     128.24   P2P (RSTP)
```

24.7. show spanning-tree mst configuration

Item	Description
Syntax	show spanning-tree mst configuration
Parameter	
Default	
Mode	Privileged EXEC
Usage	To show the global MST configuration, use the command s**how spanning-tree mst configuration** in the Privileged EXEC mode.

Example:

The following example shows the global MST configuration.

```
Switch# show spanning-tree mst configuration
Name      [Valkyrie]
Revision  1     Instances configured 3

Instance  Vlans mapped
-------------------------------------------------------------------
0         1-9,21-99,101-4094
1         10-20
```

```
2        100
-----------------------------------------------------------------
```

24.8. show spanning-tree mst interface

Item	Description
Syntax	show spanning-tree mst instance-id interface IF_PORTS
Parameter	instance-id The MSTP instance ID. Its valid range is from 0 to 15.
	interface IF_PORTS: An interface ID or the list of interface IDs.
Default	
Mode	Privileged EXEC
Usage	To show the MSTP instance information on the specific interface, use the command **show spanning-tree mst interface** in the Privileged EXEC mode.

Example:

The following example shows the MSTP 0 and 1 information individually on the interface gi23.

```
Switch# show spanning-tree mst 0 interfaces gi24
 MST Port Information
============================================================
 Instance Type : CIST (0)
------------------------------------------------------------
     Port Identifier : 128/24
  External Path-Cost : 0       /20000
 Internal Path-Cost : 0       /20000
------------------------------------------------------------
  Designated Root Bridge : 32768/00:E0:4C:00:00:00
      External Root Cost : 0
    Regional Root Bridge : 32768/00:E0:4C:00:00:00
      Internal Root Cost : 0
       Designated Bridge : 32768/00:E0:4C:00:00:00
 Internal Port Path Cost : 20000
              Port Role : Designated
             Port State : Forwarding
------------------------------------------------------------
Switch# show spanning-tree mst 1 interfaces gi24 MST Port Information
============================================================
Instance Type : MSTI (1)
------------------------------------------------------------

Port Identifier : 128/24
Internal Path-Cost : 0       /20000
```

```
-----------------------------------------------------------
Regional Root Bridge : 32768/00:E0:4C:00:00:00 Internal Root Cost : 0
Designated Bridge : 32768/00:E0:4C:00:00:00 Internal Port Path Cost : 20000
Port Role : Designated Port State : Forwarding
-----------------------------------------------------------
```

24.9. spanning-tree

Item	Description
Syntax	spanning-tree
	no spanning-tree
Parameter	
Default	Spanning-Tree is enabled by default.
Mode	Global Configuration
Usage	To enable the spanning tree, use the command **spanning-tree** in the Global Configuration mode; and use the **no** form of the command to disable the spanning tree on the switch.

Example:

The following example disables and enables the spanning tree individually.

```
Switch(config)# no spanning-tree
Switch(config)# spanning-tree
```

24.10. spanning-tree bpdu

Item	Description
Syntax	spanning-tree bpdu (filtering|flooding)
	no spanning-tree bpdu
Parameter	**filtering**: Filter the BPDU when STP is diabled.
	flooding: Flood the BPDU when the STP is disabled.
Default	The default configuration is flooding.
Mode	Global Configuration
Usage	To configure the action of Bridge Protocol Data Unit (BPDU) handlring when STP is disabled, use the command **spanning-tree bpdu** in the Global Configuration mode. To restore the configuration to the default action, use the **no** form of the command.

Example:

The following example configures the action of BPDU handling to fliter when the STP is disabled.

```
Switch(config)# spanning-tree bpdu filtering
```

24.11. spanning-tree bpdu-filter

Item	Description
Syntax	spanning-tree bpdu-filter
	no spanning-tree bpdu-filter
Parameter	
Default	BPDU filter is disabled.
Mode	Interface Configuration
Usage	To enable the BPDU filter, use the command **spanning-tree bpdu-filter** in the Interface Configuration mode; and use **no** form of the command to disable the BPDU filter.

Example:

The following example enables the BPDU filter for interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# spanning-tree bpdu-filter
```

24.12. spanning-tree bpdu-guard

Item	Description
Syntax	spanning-tree bpdu-guard
	no spanning-tree bpdu-guard
Parameter	
Default	BPDU guard is disabled
Mode	Interface Configuration
Usage	To enable the BPDU filter, use the command **spanning-tree bpdu-guard** in the Interface Configuration mode; and use **no** form of the command to disable the BPDU filter.

Example:

The following example enables the BPDU guard for interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# spanning-tree bpdu-guard
```

24.13. spanning-tree cost

Item	Description
Syntax	spanning-tree cost cost

<table>
<tr><td></td><td>no spanning-tree cost</td></tr>
<tr><td>Parameter</td><td>cost: The port path cost. For the long path cost method, its valid range is from 0 to 200000000; and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method.</td></tr>
<tr><td>Default</td><td>The default port path cost is 0, and it is determined by the port speed and the path cost method (long or short).
<table>
<tr><th>Interface</th><th>Long</th><th>Short</th></tr>
<tr><td>Gigabit Ethernet (1000Mbps)</td><td>20000</td><td>4</td></tr>
<tr><td>Fast Ethernet (100Mbps)</td><td>200000</td><td>19</td></tr>
<tr><td>Ethernet (10Mbps)</td><td>2000000</td><td>100</td></tr>
</table></td></tr>
<tr><td>Mode</td><td>Interface Configuration</td></tr>
<tr><td>Usage</td><td>To configure the STP path cost for an interface, use the command spanning-tree cost in the Interface Configuration mode; and use the no form of the command to restore it to the default configuration.</td></tr>
</table>

Example:

The following example configures port path cost to 30000 for interface gi2.

```
Switch(config)# interface gi2
Switch(config-if)# spanning-tree cost 30000
```

24.14. spanning-tree hello-time

Item	Description
Syntax	spanning-tree hello-time seconds
	no spanning-tree hello-time
Parameter	**seconds:** STP hello time in second. Its valid range is from 1 to 10 seconds.
Default	The default STP hello time is 2 seconds.
Mode	Global Configuration
Usage	STP hello time is the time interval to broadcast its hello message to other bridges. To configure the STP hello time, use the command **spanning-tree hello-time** in the Global Configuration mode; and use the **no** form of the command to restore the hello time to default configuration. When the hello time is configured, the following relationship should be maintained: Max-Age >= 2 * (hello-time + 1)

Example:

The following example configures BPDU hello time to 4.

```
Switch(config)# spanning-tree hello-time 4
```

24.15. spanning-tree edge

Item	Description
Syntax	spanning-tree edge
	no spanning-tree edge
Parameter	
Default	The default configuration is disabled.
Mode	Interface Configuration
Usage	To enable the edge mode for an interface, use the command **spanning-tree edge** in the Interface Configuration mode; and use the **no** form of the command to restore it to the default configuration. In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time.

Example:

The following example enables the edge mode for the interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# spanning-tree edge
```

24.16. spanning-tree link-type

Item	Description
Syntax	spanning-tree link-type (point-to-point|shared)
	no spanning-tree link-type
Parameter	**point-to-point:** Specify the port link type is point to point.
	shared: Specify the port link type is shared.
Default	The default configuration link type is point-to-point for the ports with full duplex configuration, and shared for the ports with half duplex settings.
Mode	Interface Configuration
Usage	To set the RSTP link-type for an interface, use the command **spanning-tree link** in the Interface Configuration mode. For the default configuration, use the **no** form of the command.

Example:

The following example configures the link-type to point-to-point for the interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# spanning-tree link-type point-to-point
```

24.17. spanning-tree max-hops

Item	Description
Syntax	spanning-tree max-hops counts
	no spanning-tree max-hops
Parameter	**counts**: Specify the number of hops in an MSTP regision before the BPDU is discarded. The valid range is 1 to 40.
Default	The default max-hops configuration is 20.
Mode	Global Configuration
Usage	To specify the number of hops for a BPDU to be forwarded in the MSTP region, use the command **spanning-tree max-hops** in the Global Configuration mode; and restore the setting to default configuration by the **no** form of the command.

Example:

The following example specifies the max hops for BPDU to 10.

```
Switch(config)# spanning-tree max-hops 10
```

24.18. spanning-tree mode

Item	Description
Syntax	spanning-tree mode (mstp|rstp|stp)
	no spanning-tree force-version
Parameter	**mstp**: Enable the Multiple Spanning Tree (MSTP) operation.
	rstp: Enable the Rapid Spanning Tree (RSTP) operation.
	stp: Enable the Spanning Tree (STP) operation.
Default	The default mode is rstp.
Mode	Global Configuration
Usage	To specify the spanning tree operation mode, use the command of **spanning-tree mode** in the Global Configuration mode. For the default configuration, use the command **no spanning-tree force-version** in the Global Configuration mode. When the switch is configured as MSTP mode, it can use STP and RSTP for the backward compatibility with switches working in STP and RSTP mode individually. For the RSTP configuration, the switch can also use STP for the switches working in the STP operation.

Example:

The following example sets the STP operation to MSTP.

```
Switch(config)# spanning-tree mode mstp
```

24.19. spanning-tree mst configuration

Item	Description
Syntax	spanning-tree mst configuration
Parameter	
Default	
Mode	Global Configuration
Usage	To enter the MST configuration mode for the MSTP configuration modification, use the command spanning-tree mst configuration in the Global Configuration mode.

Example:

The following example modifies the MSTP configuration in the MST Configuration mode.

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name Valkyrie
Switch(config-mst)# revision 1
```

24.20. spanning-tree mst cost

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td rowspan="2">Syntax</td><td>spanning-tree mst instance-id cost cost</td></tr>
<tr><td>no spanning-tree mst instance-id cost cost</td></tr>
<tr><td rowspan="2">Parameter</td><td>instance-id:Specify the instance ID. The valid range is from 0 to 15.</td></tr>
<tr><td>cost: Specify the path cost for the interfaces on the specific MSTP instance. For the long path cost method, its valid range is from 0 to 200000000; and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method.</td></tr>
<tr><td>Default</td><td>The default port path cost is 0, and it is determined by the port speed and the path cost method (long or short).
<table>
<tr><th>Interface</th><th>Long</th><th>Short</th></tr>
<tr><td>Gigabit Ethernet (1000Mbps)</td><td>20000</td><td>4</td></tr>
</table>
</td></tr>
</table>

		Fast Ethernet (100Mbps)	200000	19	
		Ethernet (10Mbps)	2000000	100	
Mode	Interface Configuration				
Usage	To configure the path cost for MSTP calculations, use the command **spanning-tree mst cost** in the Interface Configuration mode. If the loop occurs, the MSTP considers the path cost when selecting the interface into the Forwarding state. For the default configuration, use the **no** form of the command. When configuring the path cost on the CIST (instance 0), it is equal to the command **spanning-tree cost** in the Interface Configuration mode.				

Example:

The following example configures the path cost of interface gi1 on the instance 1 to 30000

```
Switch(config)# interface gi1
Switch(config-if)# spanning-tree mst 1 cost 30000
```

24.21. spanning-tree mst port-priority

Item	Description
Syntax	spanning-tree mst instance-id port-priority priority
	no spanning-tree mst instance-id port-priority
Parameter	**instance-id:** Specify the instance ID. The valid range is from 0 to 15.
	priority: Specify the interface priority on the specific instance.
Default	The default port priority on each instance is 128.
Mode	Interface Configuration
Usage	To configure the interface priority on the specific instances, use the command **spanning-tree mst port-priority** in the Interface Configuration mode. For the default configuration, use the **no** form of the command. The priority value must be the multiple of 16. When the port priority on the CIST (instance 0) is configured, it is equal to the command spanning-tree port-priority in the Interface Configuration mode.

Example:

The following example sets the port priority of gi1 on the instance 1 to 144;and set the port priority of gi1 on the CIST (instance 0) to 96

```
Switch(config)# interface gi1
Switch(config-if)# spanning-tree mst 1 port-priority 144
```

```
Switch(config-if)# spanning-tree mst 0 port-priority 96
```

24.22. spanning-tree mst priority

Item	Description
Syntax	spanning-tree mst instance instance-id priority priority
	no spanning-tree mst instance instance-id priority
Parameter	**instance-id**: Specify the instance ID. The valid range is from 0 to 15.
	priority: Specify the bridge priority on the specific instance. The valid range is from 0 to 61440. It nsures the probility that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge.
Default	The default priority on each instance is 32768.
Mode	Global Configuration
Usage	To configure the bridge priority on the specific instance, use the command **spanning-tree mst priority** in the Global Configuration mode. To restore the default configuration, use the **no** form of the command. The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. For the configuration of bridge priority on the CIST (instance 0), it is equal to the command **spanning-tree priority** in the Global Configuration mode.

Example:

The following example modifies the bridge priority to 4096 on instance 0 and instance 1 individually.

```
Switch(config)# spanning-tree mst 0 priority 4096
Switch(config)# spanning-tree mst 1 priority 4096
```

24.23. spanning-tree pathcost method

Item	Description
Syntax	spanning-tree pathcost method (long|short)
Parameter	**long**: The range for the path cost is from 1 to 200000000.
	short: The range for the path cost is from 1 to 65535.
Default	The default path cost method is long.
Mode	Global Configuration
Usage	To set the spanning tree path cost method, use the command **spanning-tree pathcost method** in the Global Configuration mode. If the short method is specified, the switch calculates the path cost in the range 1 throuth 65535; Otherwise, it calculates the path cost in the range 1 to

	200000000.

Example:

The following example modifies path cost method to short.

```
Switch(config)# spanning-tree pathcost method short
```

24.24. spanning-tree port-priority

Item	Description
Syntax	spanning-tree port-priority priority
	no spanning-tree port-priority priority
Parameter	**priority:** Specify the priority for an interface. The valid range is from 0 to 240.
Default	The default priority for each interface is 128.
Mode	Interface Configuration
Usage	To configure the STP priority for an interface, use the command **spanning-tree port-priority** in the Interface Configuration mode. For the default configuration, use the **no** form of the command. The priority value must be the multiple of 16.

Example:

The following example modifies the port priority to 96 for the interface gi2 .

```
Switch(config)# interface gi2
Switch(config-if)# spanning-tree port-priority 96
```

24.25. spanning-tree priority

Item	Description
Syntax	spanning-tree priority priority
	no spanning-tree priority
Parameter	**instance-id**:Specify the instance ID. The valid range is from 0 to 15.
	priority: Specify the bridge STP priority. The valid range is from 0 to 61440. It nsures the probility that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge of the STP topology.
Default	The default priority for the switch 32768.
Mode	Global Configuration
Usage	To configure the bridge priority, use the command **spanning-tree mst priority** in the Global Configuration mode. To restore the default configuration, use the **no** form of the command. The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. When swithes with the same

	priority configuration in the environment, the switch with lowest MAC address would be selected as the root bridge.

Example:

The following example modifies the bridge priority to 4096.

```
Switch(config)# spanning-tree priority 4096
```

24.26. spanning-tree tx-hold-count

Item	Description
Syntax	spanning-tree tx-hold-count count
	no spanning-tree tx-hold-count
Parameter	**count**: Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Default	The default value is 6.
Mode	Global Configuration
Usage	To limit the maximum numbers of packets transmission per second, use the command **spanning-tree tx-hold-count** in the Global Configuration mode. For the default configuration, use the **no** form of the command.

Example:

The following example sets the tx-hold-count to 4.

```
Switch(config)# spanning-tree tx-hold-count 4
```

24.27. clear spanning-tree

Item	Description
Syntax	clear spanning-tree interfaces IF_PORTS statistics
Parameter	interfaces IF_PORTS:specifies a port list to set .
Default	Spanning-Tree is enabled by default.
Mode	Privileged EXEC
Usage	Use the command **clear spanning-tree** to clear the specified port statistics

Example:

The following example clears the spanning-tree statistics on the interface gi1.

```
Switch# clear panning-tree interfaces gi1 statistics
```

24.28. spanning-tree forward-delay

Item	Description
Syntax	spanning-tree forward-delay <4-30>
	no spanning-tree forward-delay
Parameter	<4-30>:Forward-delay interval
Default	
Mode	Global configuration
Usage	Use the command **spanning-tree forward-delay** to set configuration spanning-tree forward delay. Use the **no** form of this command to restore to default setting.

Example:

This example shows how to show storm spanning-tree forward-delay.

```
Switch(config)# spanning-tree forward-delay 20
```

24.29. spanning-tree mcheck

Item	Description
Syntax	spanning-tree mcheck
Parameter	
Default	
Mode	interface configuration
Usage	Use the command **spanning-tree mcheck** to set the mcheck for specified port to migrate.

Example:

This example shows how to show storm spanning-tree mcheck for specified port to migrate test.

```
Switch(config-if)# spanning-tree mcheck
```

25. Storm Control

25.1. show storm-control

Item	Description
Syntax	show storm-control
	show storm-control interface IF_PORTS
Parameter	IF_PORTS Specify port to show.
Default	No default value for this command
Mode	Privileged EXEC
Usage	Use "**show storm-control**" command to show all storm control related configurations including global configuration and per port configurations. Use "**show storm-control interface**" command to show selected port storm control configurations.

Example:

This example shows how to show storm control global configuration.

```
Switch# show storm-control
Storm control preamble and IFG: Excluded Storm control unit: kbps
.....................................
```

This example shows how to show current storm control configuration on interface gi1

```
Switch# show storm-control interfaces gi1

Port| State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast | Action
    |       |     kbps    |        kbps        |      kbps       |
----+-------+-------------+--------------------+-----------------|------
gi1   disable   Off(10000)     Off(10000)          Off(10000)       Drop
```

25.2. storm-contro

Item	Description
Syntax	storm-control
	no storm-control
	storm-control (broadcast | unknown-unicast | unknown-multicast)
	no storm-control (broadcast | unknown-unicast | unknown-multicast)
Parameter	**broadcast**: Select broadcast storm control type
	unknown-unicast: Select unknown unicast storm control type
	unknown-multicast: Select unknown multicast storm control type

Default	Default storm control is disabled. Default broadcast storm control is disabled. Default unknown multicast storm control is disabled Default unknown unicast storm control is disabled
Mode	Interface Configuration
Usage	Storm control function is able to enable/disable on each single port. Use the "**storm control**" command to enable storm control feature on the selected ports. And use "no storm control" command to disable storm control feature. Not only port is able to enable/disable on the port. Each storm control type is also able to enable/disable on each single port. Use the "**storm-control (broadcast|unknown-unicast|unknown-multicast)**" command to enable the storm control type you need and use **no** form to disable it.

Example:

This example shows how to enable storm control on interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control
```

This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control broadcast
```

This example shows how to show current storm control configuration on interface gi1

```
Switch# show storm-control interfaces gi1
Port| State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast | Action
    |       |     kbps    |        kbps        |      kbps       |
----+-------+-------------+--------------------+-----------------|------
gi1   disable   Off(10000)     Off(10000)          Off(10000)       Drop
```

25.3. storm-control action

Item	Description
Syntax	storm-control action (drop | shutdown)
	no storm-control action
Parameter	**drop:** Drop packets after exceed storm control threshold
	shutdown: Shut down port after exceed storm control threshold
Default	Default storm control action is drop.
Mode	Interface Configuration
Usage	Use "**storm-control action**" command to set the action when the received storm control packets exceed the maximum rate on an interface. Use **no** form to restore to default action.

Example:

This example shows how to configure storm control action to shutdown port on interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control action shutdown
```

This example shows how to show storm control action on interface gi1.

```
Switch# show storm-control interfaces gi1
Port| State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast | Action
    |       |     kbps    |       kbps         |      kbps       |
----+-------+-------------+--------------------+-----------------|------
gi1   disable   Off(10000)     Off(10000)          Off(10000)     shutdown
```

25.4. storm-control ifg

Item	Description
Syntax	storm-control ifg (include | exclude)
Parameter	**include**:Include preamble & IFG (20 bytes) when count ingress storm control rate.
	exclude: Exclude preamble & IFG (20 bytes) when count ingress storm control rate
Default	Default storm control inter frame gap is excluded.
Mode	Global Configuration
Usage	Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. Use **storm-control ifg** command to include/exclude the preamble and inter frame gap into the calculating.

Example:

This example shows how to configure storm inter frame gap to include.

```
Switch(config)# storm-control ifg include
```

This example shows how to show storm control global configuration.

```
Switch# show storm-control
    Storm control preamble and IFG: Included
Storm control unit: kbps
.....................................
```

25.5. storm-control level

Item	Description
Syntax	storm-control (broadcast | unknown-unicast | unknown-multicast) level <1-1000000>
	no storm-control (broadcast | unknown-unicast | unknown-multicast) level
Parameter	**broadcast**: Select broadcast storm control type
	unknown-unicast: Select unknown unicast storm control type
	unknown-multicast: Select unknown multicast storm control type
	level <1-1000000>: Specify the storm control rate for selected type.For bps, range is 16-1000000 For pps, range is 1-262143
Default	Default broadcast storm control rate is 10000. Default unknown multicast storm control rate is 10000. Default unknown unicast storm control rate is 10000.
Mode	Interface Configuration
Usage	Each control type is allowed to have different storm control rate. Use "**storm-control (broadcast|unknown-unicast|unknown-multicast) level**" command to configure it Use **no** form to restore to default rate

Example:

This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control broadcast
Switch(config-if)# storm-control broadcast level 160
```

This example shows how to show current storm control configuration on interface gi1

```
Switch# show storm-control interfaces gi1
Port| State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast | Action
    |       |     kbps    |        kbps        |      kbps       |
----+-------+-------------+--------------------+-----------------|------
gi1   disable       160       Off(10000)          Off(10000)     shutdown
```

25.6. storm-control unit

Item	Description
Syntax	storm-control unit (kbps | pps)
Parameter	**kbps**: Storm control rate calculates by octet-based
	pps: Storm control rate calculates by packet-based
Default	Default storm control unit is bps
Mode	Global Configuration

Usage	Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. Use **storm-control unit** command to change the unit of calculating method.

Example:

This example shows how to configure storm control rate unit as pps.

```
Switch(config)# storm-control unit pps
```

This example shows how to show storm control global configuration.

```
Switch# show storm-control
Storm control preamble and IFG: Included Storm control unit: pps
    ......................................
```

26. System File

26.1. boot system

Item	Description
Syntax	boot system (image0 | image1)
Parameter	**image0:** Boot from flash image partition 0
	image1: Boot from flash image partition 1
Default	Default boot image is image0.
Mode	Global Configuration
Usage	Dual image allow user to have a backup image in the flash partition. Use "**boot system**" command to select the active firmware image. And another firmware image will become a backup one.

Example:

This example shows how to select image1 as active image.

```
Switch(config)# boot system image0
The image already be selected
```

This example shows how to show active image partition.

```
Switch# show flash
       File Name           File Size       Modified
----------------------- --------------- -----------------------
 startup-config          2660            1970-01-01 00:00:46
 rsa2                    1679            1970-01-01 02:21:55
 dsa2                    668             1970-01-01 02:22:02
 ssl_cert                916             1970-01-01 00:00:39
 image0 (active)         8275248         2021-01-20 16:55:35
 image1 (backup)         0
```

26.2. Copy

Item	Description
Syntax	copy (flash:// | tftp://) (flash:// | tftp://)
	copy tftp:// (backup-config | running-config | startup-config)
	copy (backup-config | running-config | startup-config) tftp://
	copy (backup-config | startup-config) running-config
	copy (backup-config | running-config) startup-config
	copy (running-config | startup-config) backup-config
Parameter	**flash:**//: Specify the file stored in flash to operation. Available files are:

	flash://startup-config ,flash://backup-config, flash://rsa1 flash://rsa2, flash://dsa2 ,flash://image0 ,flash://image1 flash://ram.log ,flash://flash.log
	tftp:// : Specify remote tftp server and remote file name. The format is "tftp://192.168.1.111/remote_file_name"
	running-config：Running configuration file
	startup-config: Startup configuration file
	backup-config: Backup configuration file
Default	No default value for this command.
Mode	Privileged EXEC
Usage	There are many types of files in system. These files are very important for administrator to manage the switch. The most common file operation is copy. By using these copy commands, we can upgrade, backup following type of files. 1.Firmware Image 2.Configuration Files 3.Syslog Files 4.Language Files 5.Security Certificate

Example:

This example shows how to copy running configuration to startup configuration.

```
Switch# copy running-config startupst-config
```

This example shows how to backup running configuration to remote tftp server 192.168.111 with file name test1.cfg.

```
Switch# copy running-config tftp://192.168.1.111/test1.cfg
Uploading file...Please Wait... Uploading Done
```

This example shows how to upgrade startup configuration from remote tftp server 192.168.1.111 with file name test2.cfg.

```
Switch# copy tftp://192.168.1.111/test2.cfg startup-config
Downloading file...Please Wait... Downloading Done
Upgrade config success. Do you want to reboot now? (y/n)n
```

This example shows how to backup security file dsa2 to remote tftp server 192.168.1.111 with file name dsa2.

```
Switch# copy flash://dsa2 tftp://192.168.1.111/dsa2
Uploading file...Please Wait... Uploading Done
```

26.3. delete

Item	Description
Syntax	delete (startrup-config | backup-config | flash://)
	delete system (image0 | image1)
Parameter	**flash://**: Specify the configuration file stored in flash to delete. Available files are:flash://startup-config flash://backup-config
	startup-config: Delete startup configuration file
	backup-config: Delete backup configuration file
	image0: Delete flash image0.
	image1: Delete flash image1.
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "delete" command to delete configuration files or use "**delete system**" command to delete firmware image stored in flash. The "**delete startup-config**" command is using to restore factory default and it is equal to command "**restore-defaults**".

Example:

This example shows how to delete backup configuration file.

```
Switch# delete backup-config
```

This example shows how to delete backup firmware image from flash.

```
Switch# delete system image1
It may take a few minutes to finish. Please wait...
Delete "image1" Success
```

This example shows how to show file status in flash.

```
Switch# show flash
            File Name           File Size             Modified
      ------------------- ---------------- ------------------------
         startup-config          3382            1970-01-01 01:30:18
         rsa2                    1679            1970-01-01 02:21:55
         dsa2                    668             1970-01-01 02:22:02
         ssl_cert                916             1970-01-01 00:00:39
         image0 (active)         8275248         2021-01-20 16:55:35
         image1 (backup)         0
```

26.4. restore-defaults

Item	Description
Syntax	restore-defaults [interfaces IF_PORTS]
Parameter	**interfaces IF_PORTS:** Specify port to restore its' ruuning config
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**restore-defaults**" command to restore factory default of all system. The command is equal to "**delete startup-config**".

Example:

This example shows how to restore factory defaults.

```
Switch# restore-defaults
 Restore Default Success. Do you want to reboot now? (y/n)n
```

26.5. save

Item	Description
Syntax	save
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**save**" command to save running configuration to startup configuration file. This command is equal to "**copy running-config startup-config**".

Example

This example shows how to save running configuration to startup configuration.

```
Switch# save Success
```

This example shows how to show startup configuration

```
Switch# show startup-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: Switch TS928F Switch
! System Version: v1.0.0x
! System Name: Switch
! System Up Time: 0 days, 0 hours, 0 mins, 46 secs
!
!
!
!
username "admin" secret encrypted
```

```
MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM=
        ……
```

26.6. show bootvar

Item	Description
Syntax	show bootvar
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show bootvar**" command to show image information in both flash partitions. It also shows current active image and active image on next booting.

Example:

This example shows how to show dual image information

```
Switch# show bootvar
Image    Version          Date                  Status       File Name
-----  ----------   --------------------   -----------  ----------
0          1.0.0x    2021-01-20 16:55:35     Active*
1                                            Not active

"*" designates that the image was selected for the next boot
```

26.7. show config

Item	Description
Syntax	show (running-config | startrup-config | backup-config)
	show running-config interfaces IF_PORTS
Parameter	**running-config:** Show running configuration on terminal
	startup-config: Show startup configuration on terminal
	backup-config: Show backup configuration on terminal
	IF_PORTS: Specify port to show its' ruuning config
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Our configuration file is text based. Therefore, we can show the configuration on terminal and read it by this command. Use "**show **-config**" command to show configuration files stored in system. Use "**show config interfaces**" command to show specific port configurations.

Example:

This example shows how to show startup configuration

```
Switch# show startup-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: Switch TS928F Switch
! System Version: v1.0.0x
! System Name: Switch
! System Up Time: 0 days, 0 hours, 0 mins, 46 secs
!
!
!
!
username "admin" secret encrypted
MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM=
.............................
```

This example shows how to show running configuration

```
Switch# show running-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: Switch TS928F Switch
! System Version: v1.0.0x
! System Name: Switch
! System Up Time: 0 days, 0 hours, 7 mins, 34 secs
!
!
!
!
username "admin" secret encrypted
MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM=
.....................................................
```

This example shows how to display running configuraiton on specific port.

```
Switch# show running-config interfaces gi1
interface gi1
```

26.8. show flash

Item	Description
Syntax	show flash
Parameter	
Default	No default value for this command.
Mode	Privileged EXEC
Usage	Use "**show flash**" command to show all files' status which stored in flash.

Example:

This example shows how to show all files status stored in flash.

```
Switch# show flash
            File Name            File Size        Modified
        ---------------- ---------------- ------------------------
         startup-config         2660             1970-01-01 00:00:46
         rsa2                   1675             1970-01-01 00:00:15
         dsa2                   668              1970-01-01 00:00:25
         ssl_cert               916              1970-01-01 00:00:29
         image0 (active)        8275248         2021-01-20 16:55:35
         image1 (backup)        0
```

27. Time

27.1. clock set

Item	Description
Syntax	clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2035>
Parameter	**HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)<1-31><2000-2035>**:Specify static time of year, month, day, hour, minute,second
Default	No default is defined. The clock set to 2000/01/01 08:00:00 by default at startup.
Mode	Privileged EXEC
Usage	Use the **clock set** command to set static time. The static time won't save to configuration file. You can verify your setting by entering the **show clock** Privileged EXEC command.

Example:

The example shows how to set static time of switch.

```
switch# clock set 11:03:00 sep 21 2012
2021-09-21 03:03:00 UTC+8
switch# show clock
2021-09-21 03:03:19 UTC+8
Time set manually
```

27.2. clock timezone

Item	Description
Syntax	clock timezone ACRONYM HOUR-OFFSET [minutes <0-59>]
	no clock timezone
Parameter	**ACRONYM:** Specify acronym name of time zone
	HOUR-OFFSET: Specify hour offset of time zone
	Minutes <1-59>: Specify minute offset of time zone
Default	Default time zone is UTC+8.
Mode	Global Configuration
Usage	Use the **clock timezone** command to set timezone setting. Use the **no** form of this command to restore to default setting. You can verify your setting by entering the **show clock detail** Privileged EXEC command.

Example:

The example shows how to set time zone of switch and then restore to default time zone.

```
switch(config)# clock timezone test +5
switch# show clock detail
10:13:27 2021-09-21 03:04:23 test(UTC+5)
Time set manually

Time zone:
Acronym is test
Offset is UTC+5

switch(config)# no clock timezone
switch# show clock detail
2021-09-21 03:06:22 UTC+8
Time set manually

Time zone:
Acronym is
Offset is UTC+8
```

27.3. clock source

Item	Description
Syntax	clock source (local|sntp)
Parameter	**local**: Specify to use static time
	sntp: Specify to use sntp time
Default	Default is using local time.
Mode	Global Configuration
Usage	Use the **clock source** command to set the source of time. Use the **no** form of this command to restore to default setting. You can verify your setting by entering the **show clock detail** Privileged EXEC command.

Example:

The example shows how to set clock source of switch.

```
switch(config)# clock source sntp
switch# show clock detail
2021-09-21 03:07:30 UTC+8
Time source is sntp

Time zone:
```

```
Acronym is
Offset is UTC+8
```

27.4. clock summer-time

Item	Description
Syntax	clock summer-time ACRONYM date (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM [<1-1440>]
	clock summer-time ACRONYM recurring (usa|eu) [<1-1440>]
	clock summer-time ACRONYM recurring (<1-5>|first|last)(sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM (<1- 5>|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM [<1-1440>
	no clock summer-time
Parameter	**ACRONYM:** Specify acronym name of time zone
	(jan|feb|mar|apr| may|jun|jul|aug|sep| oct|nov|dec) <1-31><2000-2037> HH:MM(jan|feb|mar|apr| may|jun|jul|aug|sep| oct|nov|dec) <1-31> <2000-2037> HH:MM: Specify non-recurring daylight saving time duration.
	<1-1440>: Specify adjust offset of daylight saving time
	usa: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November
	eu: Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October.
	(<1-5>|first|last) (sun|mon| tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun| jul|aug|sep|oct|nov|dec) HH:MM (<1-5>|first|last)(sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may| jun|jul|aug|sep|oct|nov|dec)HH:MM: Specify ecurring daylight saving time duration.
Default	No default daylight saving time is defined.
Mode	Global Configuration
Usage	Use the **clock summer-time** command to set daylight saving time for system time. The "**usa**" or "**eu**" means that use the global daylight saving policy which defined by international organization. In both the "**date**"and "**recurring**", the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The "**recurring**" means that adjust time every year within the month. Use the **no** form of this command to default setting. You can verify your setting by entering the **show clock detail** Privileged EXEC command

Example:

The example shows how to set clock summer time of switch. You can verify settings by the following show show clock command.

```
switch(config)# clock summer-time test recurring usa
switch# show clock detail
2021-09-21 06:46:39 test(UTC+9)
Time source is sntp

Time zone:
Acronym is
Offset is UTC+8

Summertime:
Acronym is test
Recurring every year.
Begins at 2 0 3 2:0
Ends at 1 0 11 2:0
Offset is 60 minutes.
```

27.5. show clock

Item	Description
Syntax	show clock [detail]
Parameter	**detail**: Show more detail information of clock
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show clock** command to show clock of switch. The “detail” means that show more information of clock such as time zone and daylight saving time.

Example:

The example shows how to show clock of switch and detail information.

```
Switch(config)# clock source sntp
Switch(config)# clock summer-time DLS recurring usa
Switch(config)# sntp host 192.168.1.100
Switch# show clock

2021-09-21 06:49:12 DLS(UTC+9)
Time source is sntp

Switch# show clock detail
2021-09-21 06:49:46 DLS(UTC+9)
Time source is sntp
```

```
Time zone:
Acronym is
Offset is UTC+8

Summertime:
Acronym is DLS
Recurring every year.
Begins at 2 0 3 2:0
Ends at 1 0 11 2:0
Offset is 60 minutes.
```

27.6. sntp

Item	Description
Syntax	sntp host HOSTNAME [port <1-65535>]
	no sntp
Parameter	**HOSTNAME:** Specify ip address or hostname of sntp server
	sntp: Specify server port of sntp server
Default	No default SNTP server defined. Default server port is 123 when server created.
Mode	Global Configuration
Usage	Use the **sntp** command to set remote SNTP server. Use the **no** form of this command to default setting. You can verify your setting by entering the show sntp Privileged EXEC command.

Example:

The example shows how to set remote SNTP server of switch.

```
switch(config)# clock source sntp
switch(config)# sntp host 192.168.1.100
switch# show sntp
SNTP is Enabled
SNTP Server address: 192.168.1.100 SNTP Server port: 123
```

27.7. show sntp

Item	Description
Syntax	show sntp
Parameter	

Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show sntp** command to remote SNTP server information.

Example:

The example shows how to show remote SNTP server.

```
Switch# show sntp
SNTP is Enabled
SNTP Server address: 192.168.1.100 SNTP Server port: 123
```

28. UDLD

28.1. errdisable recovery cause udld

Item	Description
Syntax	errdisable recovery cause udld
	no errdisable recovery cause udld
Parameter	
Default	Error disable auto recovery is disabled by default.
Mode	Global EXEC
Usage	Use the **errdisable recovery cause udld** to enable auto recovery of UniDirectional Link Detection (UDLD). Use the "**no**" to disable it.

Example:

The example shows how to enable auto recovery of UniDirectional Link Detection (UDLD).

```
switch(config)# errdisable recovery cause udld
switch# show errdisable recovery
ErrDisable Reason Timer Status
----------------------+---------------
           Bpduguard    | disabled
           Udld         |  enabled
           …
```

28.2. udld

Item	Description
Syntax	udld
	no udld
Parameter	
Default	UDLD is disabled by default.
Mode	Interface Configuration
Usage	Use the **udld** command to enable UniDirectional Link Detection (UDLD) normal mode of interface. Use the **no** form of this command to restore to default setting. You can verify your setting by entering the show udld interface Privileged EXEC command.

Example:

The example shows how to enable UniDirectional Link Detection (UDLD) normal mode

in interface gi1.

```
switch(config)# interface gi1
switch(config-if)# udld
switch# show udld interfaces gi1
Interface gi1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

28.3. udld aggressive

Item	Description
Syntax	udld aggressive
	no udld aggressive
Parameter	
Default	UDLD aggressive mode is disabled by default.
Mode	Interface Configuration
Usage	Use the **udld aggressive** command to enable UniDirectional Link Detection (UDLD) aggressive mode of interface. Use the **no** form of this command to restore to default setting. You can verify your setting by entering the show udld interface Privileged EXEC command

Example:

The example shows how to enable udld aggressive mode in interface gi1.

```
switch(config)# interface gi1
switch(config-if)# udld aggressive
switch# show udld interfaces gi1
Interface gi1
---
Port enable administrative configuration setting: Enabled / in aggressive
mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

28.4. udld message time

Item	Description
Syntax	udld message time message-time-interval
Parameter	**message-time-interval:** Specify the interval for sending message.Range is 1-90 seconds.
Default	Default interval is 15 seconds.
Mode	Global Configuration
Usage	Use the **udld message time** to set interval of UniDirectional Link Detection (UDLD) sent message.

Example:

The example shows how to set interval of UniDirectional Link Detection(UDLD) message.

```
switch(config)# udld message time 30
```

28.5. udld reset

Item	Description
Syntax	udld reset
Parameter	
Default	No default is defined.
Mode	Privileged EXEC
Usage	Use the **udld reset** command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again. If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected

Example:

The example shows how to reset all interfaces disabled by UDLD

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

28.6. show udld

Item	Description
Syntax	show udld
	show udld interfaces IF_NMLPORTS
Parameter	**IF_NMLPORTS:** Specify the normal interfaces to display udld information
Default	No default is defined
Mode	Privileged EXEC
Usage	Use the **show udld** command to to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

Example:

The example shows how to show UniDirectional Link Detection (UDLD)settings and operational status of interface gi1.

```
Switch# show udld interfaces gi1
Interface gi1
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

29. VLAN

29.1. vlan

Item	Description
Syntax	vlan
	no vlan
	show surveillance-vlan
	show surveillance-vlan interfaces IF_PORTS
Parameter	**IF_PORTS:** Specify interface is to show
Default	VLAN 1 created by default
Mode	Global Configuration Privileged EXEC
Usage	Use the **vlan** global configuration command to create VLAN. Use the **no** form of this command to remove exist VLAN. You can verify your setting by entering the **show vlan** Privileged EXEC command.

Example:

The following example creates and removes a VLAN entry (100).

```
Switch# configure
Switch (config)# vlan 100
 Switch# show vlan
VID  | VLAN Name |    Untagged Ports      | Tagged Ports  |  Type
-----+-----------+------------------------+---------------+---------
1    |   default |    gi1-24,xgi1-4,lag1-8 |           --- | Default
100  |  VLAN0100 |                    --- |           --- | Static
```

29.2. show vlan protocol-vlan

Item	Description
Syntax	show vlan protocol-vlan [group <1-8>]
	show vlan protocol-vlan interfaces IF_PORTS
Parameter	**[group <1-8>]**:Specify protocol-vlan group number
	interfaces IF_PORTS:Select port to show qos configurations.
Default	No default is defined
Mode	Privileged EXEC
Usage	This command will display protocol-vlan information.

Example:

The following example shows the configuration of protocol-vlan.

```
Switch# show vlan protocol-vlan group 1
    Group ID    |     Status    |      Type      |       value
--------------+---------------+----------------+-----------------
      1        |  Disabled     |       --       |        --
Switch# show vlan protocol-vlan interfaces gi1
Port gi1 :
  Group 1
    Status      : Disabled
  Group 2
    Status      : Disabled
  Group 3
    Status      : Disabled
  Group 4
    Status      : Disabled
  Group 5
    Status      : Disabled
  Group 6
    Status      : Disabled
  Group 7
    Status      : Disabled
  Group 8
    Status      : Disabled
```

29.3. vlan protocol-vlan group(global)

Item	Description
Syntax	vlan protocol-vlan group <1-8> frame-type (ethernet_ii|llc_other|snap_1042) protocol-value VALUE
	no vlan protocol-vlan group <1-8>
Parameter	**[group <1-8>]**:Specify protocol-vlan group number
	ethernet_ii:Specify the protocol type Ethernet II
	llc_other:Specify the protocol type 802.3 LLC other
	snap_1042:Specify the protocol type 802.3 SNAP 1042
	VALUE:Protocol value (0x0600-0xFFFE)
Default	No default is defined
Mode	Global configuration
Usage	Use the **vlan protocol-vlan group frame-type protocol-value** command to set protocol-vlan of group. Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of protocol-vlan.

```
Switch(config)# vlan protocol-vlan group 1 frame-type ethernet_ii
protocol-value 0x700
```

29.4. vlan protocol-vlan group(interface)

Item	Description
Syntax	vlan protocol-vlan group <1-8> vlan <1-4094>
	no vlan protocol-vlan group <1-8>
Parameter	**[group <1-8>]**:Specify protocol-vlan group number
	<1-4094>:Specify the VLAN ID
Default	No default is defined
Mode	interface configuration
Usage	Use the **vlan protocol-vlan group vlan** command to set protocol-vlan of group. Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of protocol-vlan.

```
Switch(config-if)# switchport mode hybrid
Switch(config-if)# vlan protocol-vlan group 1 vlan 1
```

29.5. management-vlan vlan

Item	Description
Syntax	management-vlan vlan <1-4094>
	no management-vlan
Parameter	**<1-4094>**:Specify the VLAN ID
Default	default vlan is 1
Mode	global configuration
Usage	Use the **management-vlan vlan** command to set management-vlan. Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of management-vlan.

```
Switch(config)# management-vlan vlan 1
```

29.6. surveillance-vlan vlan

Item	Description
Syntax	surveillance-vlan vlan <2-4094>
	surveillance-vlan
	no surveillance-vlan
	no surveillance-vlan vlan
Parameter	**<1-4094>**:Specify the VLAN ID
Default	
Mode	global configuration
Usage	Use the **surveillance-vlan vlan** or **surveillance-vlan** command to set surveillance VLAN vid config. Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of surveillance-vlan.

```
Switch(config)# surveillance-vlan
Switch(config)# surveillance-vlan vlan 2
```

29.7. surveillance-vlan cos

Item	Description
Syntax	surveillance-vlan cos <0-7>
	no surveillance-vlan cos
Parameter	**<0-7>**: Specify the cos value .
Default	default cos is 6
Mode	global configuration
Usage	Use the **surveillance-vlan cos** command to set surveillance VLAN priority config. Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of surveillance VLAN priority.

```
Switch(config)# surveillance-vlan cos 3
```

29.8. surveillance-vlan oui-table

Item	Description
Syntax	surveillance-vlan oui-table A:B:C [DESCRIPTION]

	no surveillance-vlan oui-table A:B:C
Parameter	**A:B:C**: OUI address(xx:xx:xx)
	[DESCRIPTION]: OUI description string
Default	
Mode	global configuration
Usage	Use the **surveillance-vlan oui-table** command to set surveillance VLAN OUI config. Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of surveillance VLAN OUI.

```
Switch(config)# surveillance-vlan oui-table 00:11:22
```

29.9. surveillance-vlan aging-time

Item	Description
Syntax	surveillance-vlan aging-time <30-65536>
	no surveillance-vlan aging-time
Parameter	<30-65536>: Specify the aging time in minutes
Default	default time is1440 minutes
Mode	global configuration
Usage	Use the **surveillance-vlan aging-time** command to set surveillance vlan configuration aging value Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of surveillance vlan configuration aging value.

```
Switch(config)# surveillance-vlan aging-time 2000
```

29.10. surveillance-vlan mode

Item	Description
Syntax	surveillance-vlan mode (auto|manual)
	no surveillance-vlan mode
Parameter	**auto**: Surveillance Member Port Join Voice VLAN Automatically
	manual: Voice Member Port Join Voice VLAN Manually By Administrator
Default	
Mode	interface configuration
Usage	Use the **surveillance-vlan mode** command to set surveillance VLAN port mode setting. Use the **no** form of this command to default setting.

Example:

The following example shows the set configuration of surveillance VLAN port mode setting.

```
Switch(config-if)# surveillance-vlan mode auto
```

29.11. Name (vlan)

Item	Description
Syntax	name NAME
Parameter	NAME Specify the name of the VLAN (Max. 32 chars).
Default	Default name of new vlan is VLANxxxx. Xxxx is 4-digit vlan number.
Mode	VLAN Configuration
Usage	Use the **name vlan** configuration command to set name of vlan You can verify your setting by entering the show vlan Privileged EXEC command.

Example:

This example sets the VLAN name of VLAN 100 to be `VLAN-one-hundred`.

```
Switch(config)# vlan 100
Switch(config-vlan)# name VLAN-one-hundred
Switch# show vlan
 VID  |     VLAN Name |     Untagged Ports        |  Tagged Ports  |  Type
------+---------------+---------------------------+----------------+------
   1 |       default |      gi1-24,xgi1-4,lag1-8 |            --- | Default
 100 |VLAN-one-hundred|                       --- |            --- | Static
```

29.12. switchport mode

Item	Description
Syntax	switchport mode (access | hybrid | trunk [uplink])
	no switchport mode
Parameter	**access**: Specify the VLAN mode to Access port.
	hybrid: Specify the VLAN mode to Hybrid port.
	trunk: Specify the VLAN mode to Trunk port.
	uplink: Specify the Uplink property on this Trunk port.
Default	Default is trunk mode of all interfaces.
Mode	Port Configuration
Usage	The VLAN mode is used to configure the port for different port role. **Access port:** Accepts only untagged frames and join an untagged VLAN.

	Hybrid port: Support all functions as defined in IEEE 802.1Q specification. **Trunk port**: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. If it is an uplink port, it can recognize double tagging on this port. Use the **switch mode** port configuration command to set mode of interface You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command.

Example:

This example sets VLAN mode to Access port.

```
Switch(config)# interface gi12
Switch(config-if)# switchport mode access
Switch# show interfaces switchport gi12
Port : gi12
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled:

Port is member in:
 Vlan       Name        Egress rule
------- ------------ -----------------
   1      default      Untagged

Forbidden VLANs:
 Vlan        Name
------- ----------------------
```

29.13. switchport hybrid pvid

Item	Description
Syntax	switchport hybrid pvid <1-4094>
	no switchport hybrid pvid
Parameter	**<1-4094>:** Specify the port-based VLAN ID on the Hybrid port
Default	Default pivd is 1.
Mode	Port Configuration
Usage	Use the **switchpor hybrid pivd** port configuration command to set pvid of interface. You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command.

Example:

This example sets PVID to 100.

```
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid pvid 100
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan       Name       Egress rule
------- ----------- -----------------
  1       default       Untagged

Forbidden VLANs:
 Vlan        Name
------- ----------------------
```

29.14. switchport hybrid ingress-filtering

Item	Description
Syntax	switchport bybrid ingress-filtering
	no switchport hybrid ingress-filtering
Parameter	
Default	Default is enabled
Mode	Port Configuration
Usage	Use the **switchport hybrid ingress-filtering** port configuration command to enable vlan ingress filter. Use the **no** form of this command to disable. You can verify your setting by entering the s **show interfaces switchport** Privileged EXEC command.

Example:

This example sets ingress-filtering to disable.

```
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)#no switchport hybrid ingress-filtering
Switch# show interfaces switchport gi10
```

```
Port : gi10
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : disabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan       Name       Egress rule
------- ---------- -----------------
  1        default       Untagged

Forbidden VLANs:
 Vlan        Name
------- ----------------------
```

29.15. switchport hybrid acceptable-frame-type

Item	Description
Syntax	switchport hybrid acceptable-frame-type (all | tagged-only | untagged- only)
	no switchport hybrid acceptable-frame-type
Parameter	**all**: Specify to accept all frames.
	tagged-only: Specify to only accept tagged frames.
	untagged-only: Specify to only accept untagged frames.
Default	Default is accept all frames
Mode	Port Configuration
Usage	Use the **switchport hybrid accept-frame-type** port configuration command to choose which type of frame can be accepted. You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command

Example:

This example sets acceptable-frame-type to tagged-only.

```
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid acceptable-frame-type tagged-only
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : disabled
```

```
Acceptable Frame Type : tagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan      Name       Egress rule
------- ---------- -----------------
  1       default       Untagged

Forbidden VLANs:
 Vlan         Name
------- ----------------------
```

29.16. switchport hybrid allowed vlan

Item	Description
Syntax	switchport hybrid allowed vlan add VLAN-LIST [(tagged|untagged)]
	switchport hybrid allowed vlan remove VLAN-LIST
Parameter	**VLAN-LIST:** Specifies the VLAN list to be added or remove.
	(tagged|untagged): Specifies the member type is tagged or untagged.
Default	Only vlan 1 is untagged member by default. Default is tagged member when added.
Mode	Port Configuration
Usage	Use the **switchport hybrid allow vlan add** port configuration command to allow vlan on interface. Use the **switchport hybrid allow vlan remove** port configuration command to remove vlan on interface. You can verify your setting by entering the s **show interfaces switchport** Privileged EXEC command.

Example:

This example sets port gi10 VLAN to join the VLAN 100 as tagged member.

```
Switch(config)# interface gi10
Switch(config-if)#switchport hybrid allowed vlan add 100-105
Switch(config-if)#switchport hybrid allowed vlan remove 105
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : disabled
Acceptable Frame Type : tagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
```

```
Port is member in:
 Vlan    Name             Egress rule
------- -------------- -----------------
 1       default          Untagged
 100  VLAN-one-hundred    Tagged

Forbidden VLANs:
 Vlan       Name
------- ----------------------
```

29.17. switchport access vlan

Item	Description
Syntax	switchport access vlan <1-4094>
	no switchport access vlan
Parameter	**<1-4094>:** Specifies the access VLAN ID.
Default	Default is vlan 1
Mode	Port Configuration
Usage	Use the **switchport access vlan** port configuration command to set native vlan on interface. The vlan will be pvid on interface as well. Use the **no** form of this command to restore to default vlan You can verify your setting by entering the s **show interfaces switchport** Privileged EXEC command.

Example:

This example sets Access port gi10 native VLAN ID to 100.

```
Switch(config)# interface gi10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Access
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan    Name               Egress rule
------- ----------------- -----------------
  100    VLAN-one-hundred   Untagged
```

```
Forbidden VLANs:
 Vlan       Name
------- ----------------------
```

29.18. switchport trunk native vlan

Item	Description
Syntax	switchport trunk native vlan <1-4094>
	no switchport trunk native vlan
Parameter	**<1-4094>:** Specifies the native VLAN ID.
Default	Default is vlan 1
Mode	Port Configuration
Usage	Use the **switchport trunk native vlan** port configuration command to set native vlan on interface. Use the **no** form of this command to restore to default vlan. You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command.

Example:

This example sets Trunk port gi11 native VLAN to 100.

```
Switch(config)# interface gi11
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 100
Switch# show interfaces switchport gi11
Port : gi11
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan     Name             Egress rule
------- ----------------- -----------------
  100   VLAN-one-hundred    Untagged

Forbidden VLANs:
 Vlan       Name
------- ----------------------
```

29.19. switchport trunk allowed vlan

Item	Description
Syntax	switchport trunk allowed vlan (add | remove) (VLAN-LIST | all)
Parameter	**(add | remove):** Specify the action to add or remove the allowed VLAN list.
	(VLAN-LIST | all): Specify the VLAN list or all VLANs to be added or removed.
Default	
Mode	Port Configuration
Usage	Use the **switchport trunk allow vlan add** port configuration command to allow vlan on interface. Use the **switchport trunk allow vlan remove** port configuration command to remove vlan on interface. You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command.

Example:

This example sets Trunk port gi11 to add the allowed VLAN 100.

```
Switch(config)# interface gi11
Switch(config-if)# switchport trunk allowed vlan add 100
Switch# show interfaces switchport gi11
Port : gi11
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled: 100

Port is member in:
 Vlan     Name             Egress rule
------- ---------------- -----------------
  100  VLAN-one-hundred       Untagged

Forbidden VLANs:
 Vlan      Name
------- ----------------------
```

29.20. switchport default-vlan tagged

Item	Description
Syntax	switchport default-vlan tagged
	no switchport default-vlan tagged
Parameter	
Default	Default is untagged
Mode	Port Configuration
Usage	Use the **switchport default vlan tagged** port configuration command to become default vlan tagged member. Use the **no switchport default vlan tagged** port configuration command to restore to default You can verify your setting by entering the s**how interfaces switchport** Privileged EXEC command

Example:

This example sets Trunk port gi1 membership with the default VLAN to tag.

```
Switc(config)# interface gi1
Switch(config-if)# switchport default-vlan tagged
Switch# show interfaces switchport gi1
Port : gi1
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled:

Port is member in:
 Vlan    Name          Egress rule
------- ----------- -----------------
    1    default        Tagged

Forbidden VLANs:
 Vlan       Name
------- ----------------------
```

29.21. switchport forbidden default-vlan

Item	Description
Syntax	switchport forbidden default-vlan
	no switchport forbidden default-vlan
Parameter	
Default	Default is allowed
Mode	Port Configuration
Usage	Use the **switchport forbidden default-vlan** port configuration command to forbid default-vlan on interface. Use the **no switchport forbidden default-vlan** port configuration command to restore to default You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command

Example:

This example sets the membership of the default VLAN with port gi10 to forbidden.

```
Switch(config)# interface gi10
Switch(config-if)# switchport forbidden default-vlan
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Access
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan           Name             Egress rule
------- -------------------- -----------------
  100       VLAN-one-hundred       Untagged

Forbidden VLANs:
 Vlan           Name
------- ----------------------
   1            default
```

29.22. switchport forbidden vlan

Item	Description
Syntax	switchport forbidden vlan (add | remove) VLAN-LIST
Parameter	**(add | remove):** Add or remove forbidden membership.
	VLAN-LIST: Specify the VLAN list.
Default	No vlan is forbidden by default
Mode	Port Configuration
Usage	Use the **switchport forbidden vlan add** port configuration command to forbid vlan on interface. Use the **switchport forbidden vlan remove** port configuration command to accpet vlan on interface. You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command

Example:

This example sets the membership of the VLAN 100 with port gi10 to forbidden.

```
Switch(config)# interface gi10
Switch(config-if)# switchport forbidden vlan add 100
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Access
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 4095
Trunking VLANs Enabled:
Port is member in:
 Vlan     Name             Egress rule
------- --------------- -----------------

Forbidden VLANs:
 Vlan           Name
------- ---------------------------------
   1               default
  100      VLAN-one-hundred
```

29.23. switchport vlan tpid

Item	Description
Syntax	switchport vlan tpid (0x8100|0x88a8|0x9100|0x9200)
Parameter	**(0x8100|0x88a8|0x9100|0x9200):** Select TPID to set.
Default	Default TPID is 0x8100
Mode	Port Configuration
Usage	Use the **switchport vlan tpid** port configuration command to set TPID on interface. You can verify your setting by entering the **show running-config** Privileged EXEC command

Example:

This example sets the TPID to 0x9100 on interface gi10.

```
Switch(config)# interface gi10
Switch(config-if)# switchport mode trunk uplink
Switch(config-if)# switchport vlan tpid 0x9100
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Trunk (uplink)
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled:

Port is member in:
 Vlan          Name       Egress rule
------- --------------- -----------------
    1        default        Untagged

Forbidden VLANs:
 Vlan           Name
------- ----------------------
```

29.24. switchport tunnel vlan

Item	Description
Syntax	switchport tunnel vlan <1-4094>
	no switchport tunnel vlan

Parameter	**<1-4094>:** Specify the port-based VLAN ID on the tunne port
Default	Default vlan is 1.
Mode	Interface Configuration
Usage	Use the **switchpor tunnel vlan** port configuration command to set tunnel vlan of interface. You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command.

Example:

This example sets tunnel port gi10 native VLAN ID to 1.

```
Switch(config-if)# switchport mode tunnel
Switch(config-if)# switchport tunnel vlan 1
Switch(config-if)# do show interfaces switchport gi1
Port : gi1
Port Mode : Tunnel
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled:

Port is member in:
 Vlan           Name             Egress rule
------- ---------------------- -----------------
   1              default      Untagged

Forbidden VLANs:
 Vlan           Name
------- ----------------------
```

29.25. show vlan

Item	Description
Syntax	show vlan [(VLAN-LIST|dynamic|static)]
	show management-vlan
Parameter	**(VLAN-LIST|dynamic|static)**: Specify vlan id to show information or show all static or dynamic vlan entries.
Default	
Mode	Privileged EXEC
Usage	Display information about vlan entry

Example:

The following example specifies that show vlan

```
Switch# show vlan
VID  |  VLAN Name |  Untagged Ports        |   Tagged Ports    |  Type
-------+-----------+----------------------+------------------+--------
   1 |   default   | gi2-10,gi12-24,xgi1-4,lag1-8 |      gi1  | Default
 100 | VLAN-one-hundred |               gi1|             --- | Static
```

29.26. show vlan interface membership

Item	Description
Syntax	show vlan VLAN-LIST interfaces IF_PORTS membership
Parameter	**<VLAN-List>:** Specify vlan to show
Default	
Mode	Privileged EXEC
Usage	Display information about vlan membership on interfaces.

Example:

The following example specifies that show vlan interface membership

```
Switch# show vlan 100 interfaces gi10 membership

------------------------
 VLAN ID   : 100
 VLAN Type : Static
---------+--------------
  Port   |  Membership
---------+--------------
  gi10   |    Excluded
---------+--------------
```

29.27. show interface switchport

Item	Description
Syntax	show interface switchport interfaces IF_PORTS
Parameter	**IF_PORTS:** Specify interfaces protocol vlan to display
Default	
Mode	Privileged EXEC
Usage	The following example specifies that **show interfacce switchport**

Example:

```
Switch(config)# interface gi10
Switch(config-if)# switchport trunk allowed vlan add 100
```

```
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Trunk (uplink)
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled: 100
Port is member in:
 Vlan      Name         Egress rule
--------- ------------ -----------------
  1         default       Untagged
  100  VLAN-one-hundred  Tagged

Forbidden VLANs:
 Vlan           Name
--------- ----------------------
Vlan    Name
```

30. Voice VLAN

30.1. voice-vlan (Global)

Item	Description
Syntax	voice-vlan
	no voice-vlan
Parameter	
Default	Voice VLAN is disabled
Mode	Global Configuration
Usage	Use the **voice vlan** global configuration command to enable the functional Voice VLAN on the device. Use the **no** form of this command to disable voice vlan function. You can verify your setting by entering the **show voice vlan** Privileged EXEC command.

Example:

The following example shows how to enable voice vlan.

```
Switch(config)# vlan  2-3
Switch(config)# voice-vlan vlan 2
Switch(config)# voice-vlan
Switch# show voice-vlan
Administrate Voice VLAN state : disabled
Voice VLAN ID   : 2
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      6
Voice VLAN 1p Remark: disabled
```

30.2. voice-vlan (Interface)

Item	Description
Syntax	voice-vlan
	no voice-vlan
Parameter	
Default	the default all port admin-staus is disabled.
Mode	Interface Configuration
Usage	Use the **voice vlan** Interface configuration command to enable OUI voice VLAN configuration on an interface Use the **no** form of this command to disable voice vlan on an interfaces You can verify your setting by entering the **show voice vlan** Privileged EXEC

	command

Example:

The following example how to enable voice VLAN function in oui mode on an interface

```
Switch(config)#interface range gi1-3
Switch(config-if)#voice-vlan
Switch# show voice-vlan interfaces gi1-8
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 6
Voice VLAN 1p Remark: disabled

OUI table
      OUI MAC      |   Description    |  OUI Mask
---------------------+--------------+--------------------
   00:E0:BB:00:00:00   |      3COM      |  FF:FF:FF:00:00:00
   00:03:6B:00:00:00   |     Cisco      |  FF:FF:FF:00:00:00
   00:E0:75:00:00:00   |   Veritel      |  FF:FF:FF:00:00:00
   00:D0:1E:00:00:00   |   Pingtel      |  FF:FF:FF:00:00:00
   00:01:E3:00:00:00   |   Siemens      |  FF:FF:FF:00:00:00
   00:60:B9:00:00:00   | NEC/Philips    |  FF:FF:FF:00:00:00
   00:0F:E2:00:00:00   |       H3C      |  FF:FF:FF:00:00:00
   00:09:6E:00:00:00   |     Avaya      |  FF:FF:FF:00:00:00

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |    Auto     | Src
gi2    | Disabled |    Auto     | Src
gi3    |  Enabled |    Auto     | Src
gi4    | Disabled |    Auto     | Src
gi5    | Disabled |    Auto     | Src
gi6    | Disabled |    Auto     | Src
gi7    | Disabled |    Auto     | Src
gi8    | Disabled |    Auto     | Src
```

30.3. voice-vlan vlan

Item	Description
Syntax	voice-vlan vlan <2-4094>
	no voice-vlan vlan
Parameter	**<2-4094>:** Specify the voice VLAN ID
Default	The default Voice VLAN ID is None.
Mode	Global Configuration

Usage	Use the **voice vlan id** global configuration command to configure the VLAN identifier of the voice VLAN statically. Use the **no** form of this command to restore voice vlan id to default. You can verify your setting by entering the **show voice vlan** Privileged EXEC command

Example:

The following example shows how to set Voice vlan id. The vlan id must be created first.

```
Switch(config)# voice-vlan vlan 128
Switch# show voice-vlan
Administrate Voice VLAN state : enabled
Voice VLAN ID  128
Voice VLAN Aging   : 1440 minutes
Voice VLAN CoS     6
Voice VLAN 1p Remark: disabled
```

30.4. voice-vlan oui-table

Item	Description
Syntax	voice-vlan oui-table A:B:C [DESCRIPTION]
	no voice-vlan oui-table [A:B:C]
Parameter	**A:B:C**: Specify OUI Mac address to add or remove
	DESCRIPTION: Specify description of the specified MAC address to the voice VLAN OUI table
Default	The system default has 8 oui addresses.
Mode	Global Configuration
Usage	Use the **voice vlan oui-table** global configuration command to add oui mac address to OUI Table Use the **no** form of this command to remove all or specified oui mac address.. You can verify your setting by entering the **show voice vlan** Privileged EXEC command

Example:

This following example shows how to add OUI Mac.

```
Switch(config)# voice-vlan oui-table 00:01:02  "Test "
Switch# show voice-vlan interfaces gi1
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 6
Voice VLAN 1p Remark: disabled

OUI table
      OUI MAC        |   Description  |  OUI Mask
---------------------+----------------+---------------------
```

```
00:E0:BB:00:00:00   |      3COM      |  FF:FF:FF:00:00:00
  00:03:6B:00:00:00   |     Cisco      |  FF:FF:FF:00:00:00
  00:E0:75:00:00:00   |   Veritel      |  FF:FF:FF:00:00:00
  00:D0:1E:00:00:00   |   Pingtel      |  FF:FF:FF:00:00:00
  00:01:E3:00:00:00   |   Siemens      |  FF:FF:FF:00:00:00
  00:60:B9:00:00:00   | NEC/Philips    |  FF:FF:FF:00:00:00
  00:0F:E2:00:00:00   |       H3C      |  FF:FF:FF:00:00:00
  00:09:6E:00:00:00   |     Avaya      |  FF:FF:FF:00:00:00
  00:01:02:00:00:00   |      Test      |  FF:FF:FF:00:00:00

  Port |  State   | Port Mode   | Cos Mode
-------+----------+-------------+-----------
  gi1    |  Enabled |    Auto     | Src
```

30.5. voice-vlan cos (Global)

Item	Description
Syntax	voice-vlan cos <0-7> [remark]
	no voice-vlan cos
Parameter	**<0-7>:** Specify the voice VLAN Class of Service value in telephone oui mode
	remark: Specify that the L2 user priority is remarked with the CoS value
Default	The default cos value is 6, remark is disabled.
Mode	Global Configuration
Usage	Use the **voice vlan cos** global configuration command to configure the voice VLAN cos value and 1p remark function Use the **"no"** form to restore to default mode. You can verify your setting by entering the **show voice vlan** Privileged EXEC command

Example:

The following example show how to set cos value and enable 1p remark function

```
Switch(config)# voice-vlan cos 7 remark
Switch# show voice-vlan
Administrate Voice VLAN state   : enabled
Voice VLAN ID       : 2
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 7
Voice VLAN 1p Remark: enable
```

30.6. voice-vlan cos (Interface)

Item	Description
Syntax	voice-vlan cos (src | all)
	no voice-vlan cos
Parameter	**src**: Specify QoS attributes are applied to packets with OUIs in the source MAC address.
	all: Specify QoS attributes are applied to packets that are classified to the Voice VLAN.
Default	The default all port in Src mode.
Mode	Interface configuration
Usage	Use the **voice vlan cos** Interface configuration command to configure OUI voice VLAN cos mode configuration on an interface Use the "**no**" form to restore to default mode. You can verify your setting by entering the **show voice-vlan interfaces** Privileged EXEC command

Example:

The following example how to configure voice packet QoS attributes on an interface

```
Switch(config)#interface range gi1-3
Switch(config-if)#voice-vlan cos all
Switch# show voice-vlan interfaces gi1-8
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 7
Voice VLAN 1p Remark: enabled

OUI table
      OUI MAC         |   Description  |  OUI Mask
----------------------+------------------------+--------------------
   00:E0:BB:00:00:00   |      3COM      |  FF:FF:FF:00:00:00
   00:03:6B:00:00:00   |     Cisco      |  FF:FF:FF:00:00:00
   00:E0:75:00:00:00   |   Veritel      |  FF:FF:FF:00:00:00
   00:D0:1E:00:00:00   |   Pingtel      |  FF:FF:FF:00:00:00
   00:01:E3:00:00:00   |   Siemens      |  FF:FF:FF:00:00:00
   00:60:B9:00:00:00   | NEC/Philips    |  FF:FF:FF:00:00:00
   00:0F:E2:00:00:00   |       H3C      |  FF:FF:FF:00:00:00
   00:09:6E:00:00:00   |     Avaya      |  FF:FF:FF:00:00:00
   00:01:02:00:00:00   |      Test      |  FF:FF:FF:00:00:00

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |    Auto     | All
```

```
gi2    | Disabled |    Auto     | All
gi3    |  Enabled |    Auto     | All
gi4    | Disabled |    Auto     | Src
gi5    | Disabled |    Auto     | Src
gi6    | Disabled |    Auto     | Src
gi7    | Disabled |    Auto     | Src
gi8    | Disabled |    Auto     | Src
```

30.7. voice-vlan mode

Item	Description
Syntax	voice-vlan mode (auto|manual)
	no voice-vlan mode
Parameter	**auto**: Specifies that the port is identified as a candidate to join the voice VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as voice equipment is seen on the port, the port joins the voice VLAN as a tagged port.
	manual: Specifies that the port is manually assigned to the voice VLAN.
Default	The default is auto mode.
Mode	Interface configuration
Usage	Use the **voice-vlan mode** global configuration command to configure the voice VLAN mode for interface. Use the **"no"** form to restore to default mode. You can verify your setting by entering the **show voice-vlan** interfaces Privileged EXEC command.

Example:

The following example how to configure voice mode to manual

```
Switch(config)#interface range gi1-3
Switch(config-if)#voice-vlan mode manaul
Switch# show voice-vlan interfaces gi1-8
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 7
Voice VLAN 1p Remark: enabled

OUI table
      OUI MAC         |   Description  |  OUI Mask
----------------------+---------------+---------------------
   00:E0:BB:00:00:00   |      3COM      |  FF:FF:FF:00:00:00
   00:03:6B:00:00:00   |     Cisco      |  FF:FF:FF:00:00:00
   00:E0:75:00:00:00   |   Veritel      |  FF:FF:FF:00:00:00
   00:D0:1E:00:00:00   |   Pingtel      |  FF:FF:FF:00:00:00
   00:01:E3:00:00:00   |   Siemens      |  FF:FF:FF:00:00:00
```

```
   00:60:B9:00:00:00   | NEC/Philips    |  FF:FF:FF:00:00:00
   00:0F:E2:00:00:00   |      H3C       |  FF:FF:FF:00:00:00
   00:09:6E:00:00:00   |     Avaya      |  FF:FF:FF:00:00:00
   00:01:02:00:00:00   |      Test      |  FF:FF:FF:00:00:00

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |  Manual     | All
gi2    | Disabled |  Manual     | All
gi3    |  Enabled |  Manual     | All
gi4    | Disabled |    Auto     | Src
gi5    | Disabled |    Auto     | Src
gi6    | Disabled |    Auto     | Src
gi7    | Disabled |    Auto     | Src
gi8    | Disabled |    Auto     | Src
```

30.8. voice-vlan aging-time

Item	Description
Syntax	voice-vlan aing-time <30-65536>
	no voice-vlan aing-time
Parameter	**<30-65536>:** Specify the voice VLAN aging timeout interval in minutes
Default	The default aging-timeout value is 1440 minutes.
Mode	Global Configuration
Usage	Use the **voice vlan aging-time** global configuration command to configure the voice VLAN aging timeout. Use the **"no"** form to restore to default time. You can verify your setting by entering the **show voice vlan** Privileged EXEC command

Example:

The following example shows how to set aging time.

```
Switch(config)# voice-vlan aging-time 720
Switch# show voice-vlan
Administrate Voice VLAN state   : enabled
Voice VLAN ID       : 2
Voice VLAN Aging    : 720 minutes
Voice VLAN CoS      : 7
Voice VLAN 1p Remark: enabled
```

30.9. show voice-vlan

Item	Description
Syntax	show voice-vlan
	show voice-vlan interfaces [IF_PORTS]
Parameter	**IF_PORTS:** Specifies intefaces to display voice VLAN settings in oui mode
Default	
Mode	Privileged EXEC
Usage	Use the **show voice vlan** command in EXEC mode to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI

Example:

The following example show how to display voice vlan oui mode settings

```
Switch# show voice-vlan
Administrate Voice VLAN state   : enabled
Voice VLAN ID       : 2
Voice VLAN Aging    : 720 minutes
Voice VLAN CoS      : 7
Voice VLAN 1p Remark: enabled
Switch# show voice-vlan interfaces gi1-4
Voice VLAN Aging    : 720 minutes
Voice VLAN CoS      : 7
Voice VLAN 1p Remark: enabled

OUI table
       OUI MAC         |   Description  |  OUI Mask
--------------------+---------------+--------------------
   00:E0:BB:00:00:00   |      3COM      |  FF:FF:FF:00:00:00
   00:03:6B:00:00:00   |     Cisco      |  FF:FF:FF:00:00:00
   00:E0:75:00:00:00   |   Veritel      |  FF:FF:FF:00:00:00
   00:D0:1E:00:00:00   |   Pingtel      |  FF:FF:FF:00:00:00
   00:01:E3:00:00:00   |   Siemens      |  FF:FF:FF:00:00:00
   00:60:B9:00:00:00   | NEC/Philips    |  FF:FF:FF:00:00:00
   00:0F:E2:00:00:00   |       H3C      |  FF:FF:FF:00:00:00
   00:09:6E:00:00:00   |     Avaya      |  FF:FF:FF:00:00:00
   00:01:02:00:00:00   |      Test      |  FF:FF:FF:00:00:00

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |  Manual     | All
gi2    | Disabled |  Manual     | All
```

```
gi3    |  Enabled |  Manual     | All
gi4    | Disabled |    Auto     | Src
```

31. ipv6 mld

31.1. clear ipv6 mld snooping

Item	Description
Syntax	clear ipv6 mld snooping groups [(dynamic|static)]
	clear ipv6 mld snooping statistics
Parameter	**dynamic:** Specify dynamic groups
	static:Specify static groups
Default	
Mode	Privileged Configuration
Usage	This command will clear the ipv6 mld snooping groups and statistics of type.

Example:

The following example specifies that clear ipv6 mld snooping groups and statistics test.

```
Switch# clear ipv6 mld snooping groups dynamic
Switch# clear ipv6 mld snooping statistics
```

31.2. ipv6 mld snooping

Item	Description
Syntax	ipv6 mld snooping
	no ipv6 mld snooping
Parameter	
Default	
Mode	Global Configuration
Usage	Use the **ipv6 mld snooping** command to enable mld snooping function. Use the **no** form of this command to disable.

Example:

The following example specifies that set ipv6 mld snooping test.

```
Switch(config)# ipv6 mld snooping
```

31.3. ipv6 mld snooping report-suppression

Item	Description
Syntax	ipv6 mld snooping report-suppression
	no ipv6 mld snooping report-suppression

Parameter	
Default	
Mode	Global Configuration
Usage	Use the **ipv6 mld snooping report-suppression** command to enable mld snooping report-suppression function. Use the **no** form of this command to disable.

Example:

The following example specifies that set ipv6 mld snooping report-suppression test.

```
Switch(config)# ipv6 mld snooping report-suppression
```

31.4. ipv6 mld snooping unknown-multicast

Item	Description
Syntax	ipv6 mld snooping unknown-multicast action (drop|flood|router-port) no ipv6 mld snooping unknown-multicast action
Parameter	**(drop | flood | router- port):** Drop、flood in vlan or forward to router port of unknown multicast packet
Default	Default is flood.
Mode	Global Configuration
Usage	Use the **ipv6 mld snooping unknown-multicast action** command to change action. Use the **no** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping command.

Example:

The following example specifies that set ipv6 mld snooping unknown multicast action .

```
Switch(config)# ipv6 mld snooping unknown-multicast action drop
Switch# show ipv6 mld snooping
              MLD Snooping Status
              --------------------

    Snooping                     : Enabled
    Report Suppression            : Enabled
    Operation Version             : v1
    Forward Method                : mac
    Unknown IPv6 Multicast Action   : Drop
    ..............
```

31.5. ipv6 mld snooping forward-method

Item	Description
Syntax	ipv6 mld snooping forward-method (mac|dip)
Parameter	**mac**: Specify the check as mac
	dip:Specify the check as dip
Default	Default is mac
Mode	Global Configuration
Usage	Use the **ipv6 mld snooping forward-method** command to change mld lookup mode. You can verify settings by the show ipv6 mld snooping command.

Example:

The following example specifies that set ipv6 mld snooping mld lookup mode.

```
Switch(config)# ipv6 mld snooping forward-method dip
Switch# show ipv6 mld snooping
                MLD Snooping Status
                --------------------

    Snooping                      : Enabled
    Report Suppression             : Enabled
    Operation Version              : v1
    Forward Method                 : dip
    Unknown IPv6 Multicast Action   : Drop
```

31.6. ipv6 mld snooping version

Item	Description
Syntax	ipv6 mld snooping version (1|2)
Parameter	**(1|2):** mld operation version 1 or mld operation version 2 basic mode
Default	default mode of operation is 1
Mode	Global Configuration
Usage	Use the **ipv6 mld snooping version** command to set mld operation version. You can verify settings by the show ipv6 mld snooping command.

Example:

The following example specifies that set ipv6 mld operation version.

```
Switch(config)# ipv6 mld mld operation version 2
Switch# show ipv6 mld snooping
                MLD Snooping Status
```

```
--------------------

Snooping                          : Enabled
Report Suppression                 : Enabled
Operation Version                  : v2
Forward Method                     : dip
Unknown IPv6 Multicast Action      : Drop
```

31.7. ipv6 mld snooping vlan VLAN-LIST

Item	Description
Syntax	ipv6 mld snooping vlan VLAN-LIST
	ipv6 mld snooping vlan VLAN-LIST forbidden-router-port IF_PORTS
	ipv6 mld snooping vlan VLAN-LIST immediate-leave
	ipv6 mld snooping vlan VLAN-LIST static-router-port IF_PORTS
	ipv6 mld snooping vlan VLAN-LIST router learn pim-dvmrp
	ipv6 mld snooping vlan VLAN-LIST robustness-variable <1-7>
	ipv6 mld snooping vlan VLAN-LIST response-time <5-20>
	ipv6 mld snooping vlan VLAN-LIST query-interval <30-18000>
	ipv6 mld snooping vlan VLAN-LIST last-member-query-interval <1-25>
	ipv6 mld snooping vlan VLAN-LIST last-member-query-count <1-7>
	ipv6 mld snooping vlan VLAN-LIST static-port IF_PORTS
	ipv6 mld snooping vlan VLAN-LIST forbidden-port IF_PORTS
	no ipv6 mld snooping vlan VLAN-LIST [**]
Parameter	**VLAN-LIST**:specifies VLAN ID list to set.
	IF_PORTS:specifies a port list to set or remove.
	<1-7>:specifies a robustness value to set.
	<5-20>:specifies a response time to set.
	<30-18000>:specifies query interval to set.
	<1-25>:specifies last member query interval to set.
	<1-7>:specifies last member query count to set.
	[**]:Represents other options following this command
Default	
Mode	Global Configuration
Usage	Use the **ipv6 mld snooping vlan VLAN-LIST [XXXX]** command to set the functions of the MLD snooping VLAN. Use the **no** form of this command to disable.

Example:

The following example specifies that set ipv6 mld snooping vlan .

```
Switch(config)# ipv6 mld snooping vlan 2
Switch(config)# ipv6 mld snooping vlan 2 forbidden-router-port Gi1
Switch(config)# ipv6 mld snooping vlan 2 router learn pim-dvmrp
Switch(config)# ipv6 mld snooping vlan 2 robustness-variable 2
```

```
Switch(config)# ipv6 mld snooping vlan 2 response-time 5
Switch(config)# ipv6 mld snooping vlan 2 query-interval 40
Switch(config)# ipv6 mld snooping vlan 2 last-member-query-interval 2
Switch(config)# ipv6 mld snooping vlan 2 last-member-query-count 2
Switch(config)# ipv6 mld snooping vlan 2 static-port gi3
Switch(config)# ipv6 mld snooping vlan 2 forbidden-port gi4
Switch# show ipv6 mld snooping vlan
MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : enabled
MLD Snooping oper mode : enabled
MLD Snooping robustness: admin 2 oper 2
MLD Snooping query interval: admin 125 sec oper 125 sec
MLD Snooping query max response : admin 10 sec oper  10 sec
MLD Snooping last member query counter: admin 2  oper 2
MLD Snooping last member query interval: admin 1 sec  oper 1 sec
MLD Snooping immediate leave: disabled
MLD Snooping automatic learning of multicast router ports: enabled
```

31.8. ipv6 mld max-groups

Item	Description
Syntax	ipv6 mld max-groups <0-1024>
	no ipv6 mld max-groups
Parameter	**<0-1024>**: MLD snooping max group number
Default	Default is 1024
Mode	Interface configuration
Usage	Use the **ipv6 mld max-groups** command to set mld port max number of group. Use the **no** form of this command to restore to default setting.

Example:

The following example specifies that set mld port max number of group test.

```
Switch(config-if)# ipv6 mld max-groups 1
```

31.9. ipv6 mld max-groups action

Item	Description
Syntax	ipv6 mld max-groups action (deny|replace)
Parameter	**deny**:MLD max-group action deny
	replace:MLD max-group action replace
Default	The default action is deny

Mode	Interface configuration
Usage	Use the **ipv6 mld max-groups action** command to set mld port max group action. Use the **no** form of this command to restore to default setting.

Example:

The following example specifies that set mld port max group action test.

```
Switch(config-if)# ipv6 mld max-group action replace
```

31.10. ipv6 mld profile

Item	Description
Syntax	ipv6 mld profile <1-128>
	no ipv6 mld profile <1-128>
Parameter	**<1-128>**:MLD Profile index
Default	
Mode	global configuration
Usage	Use the **ipv6 mld profile** command to set configuration mld profile enter. Use the **no** form of this command to restore to default setting.

Example:

The following example specifies that set mld profile enter test.

```
Switch(config)# ipv6 mld profile 1
```

31.11. profile range ipv6

Item	Description
Syntax	profile range ipv6 X:X::X:X [X:X::X:X] action (permit|deny)
Parameter	X:X::X:X:IPv6 multicast address start
	[X:X::X:X]:IPv6 multicast address end
	permit:Action permit
	deny:Action deny
Default	
Mode	global configuration
Usage	Use the **ipv6 mld profile** command to set configuration mld profile entry set.

Example:

The following example specifies that set mld profile enter set test.

```
Switch(config-mld-profile)# profile range ipv6 ff33:33::33:33
```

```
ff33:33::33:66 action deny
    Switch(config-mld-profile)# do show ipv6 mld profile 1
    IPv6 mld profile index: 1
    IPv6 mld profile action: deny
    Range low ip: ff33:33::33:33
    Range high ip: ff33:33::33:66
```

31.12. ipv6 mld filter

Item	Description
Syntax	ipv6 mld filter <1-128>
	no ipv6 mld filter
Parameter	**<1-128>**:IPv6 filter profile index
Default	
Mode	interface configuration
Usage	Use the **ipv6 mld filter** command to set configuration mld filter content. Use the **no** form of this command to restore to default setting.

Example:

The following example specifies that set mld filter content test.

```
Switch(config-if)# ipv6 mld filter 1
```

32. rmon

32.1. rmon

Item	Description
Syntax	clear rmon interfaces IF_PORTS statistics show rmon interfaces IF_PORTS statistics
Parameter	**interfaces IF_PORTS**: Specify the ports to display information
Default	
Mode	Privileged EXEC
Usage	This command will clear the rmon interfaces statistics. You can verify settings by the **show rmon interfaces IF_PORTS statistics** command.

Example:

The following example specifies that clear rmon statistics test.

```
Switch# clear rmon interfaces gi1 statistics
Switch# show rmon interfaces gi1 statistics
==== Port gi1 ============================
etherStatsDropEvents           : 0
etherStatsOctets               : 0
etherStatsPkts                 : 0
etherStatsBroadcastPkts        : 0
etherStatsMulticastPkts        : 0
etherStatsCRCAlignErrors       : 0
etherStatsUnderSizePkts        : 0
etherStatsOverSizePkts         : 0
etherStatsFragments            : 0
etherStatsJabbers              : 0
etherStatsCollisions           : 0
etherStatsPkts64Octets         : 0
etherStatsPkts65to127Octets    : 0
etherStatsPkts128to255Octets   : 0
etherStatsPkts256to511Octets   : 0
etherStatsPkts512to1023Octets  : 0
etherStatsPkts1024to1518Octets : 0
```

32.2. show rmon event

Item	Description
Syntax	show rmon event (<1-65535>|all)
	show rmon event <1-65535> log
Parameter	<1-65535>:Specify to index of event
	all:Specify to display all events.
Default	
Mode	Privileged EXEC
Usage	This command will display rmon event info.

Example:

The following example specifies that show rmon event.

```
Switch# show rmon event all
Switch# show rmon event 2 log
Event entry not exist
```

32.3. show rmon history

Item	Description
Syntax	show rmon history (<1-65535>|all)
	show rmon history <1-65535> statistic
Parameter	**<1-65535>**:Specify to index of history
	all:Specify to display all history.
Default	
Mode	Privileged EXEC
Usage	This command will display rmon history info.

Example:

The following example specifies that show rmon history.

```
Switch# show rmon history all
Switch# show rmon history 3 statistic
History entry not exist!
```

32.4. rmon event

Item	Description
Syntax	rmon event <1-65535> [log] [trap COMMUNITY] [description DESCRIPTION] [owner NAME]

	no rmon event <1-65535>
Parameter	**<1-65535>**:Specify to index of history
	[log]:enable log for event
	COMMUNITY:community name of trap (0~31 charactors)
	DESCRIPTION:description of event (0~127 charactors)
	NAME:owner name of event (0~31 charactors)
Default	
Mode	Global configuration
Usage	Use the **rmon event log trap description owner** command to set configuration rmon event. Use the **no** form of this command to restore to default setting.

Example:

The following example specifies that set configuration rmon event test.

```
Switch(config)# rmon event 1 trap test description test1 owner test2
Switch(config)# do show rmon event 1
Rmon Event Index       : 1
Rmon Event Type        : SNMP-Trap
Rmon Event Community   : test
Rmon Event Description : test1
Rmon Event Last Sent   :  (0) 0:00:00.00
Rmon Event Owner       : test2
```

32.5. rmon alarm

Item	Description
Syntax	rmon alarm <1-65535> interface IF_PORT (drop-events|octets|pkts|broadcast-pkts|multicast-pkts|crc-align-errors|undersize-pkts|oversize-pkts|fragments|jabbers|collisions|pkts64octets|pkts65to127octets|pkts128to255octets|pkts256to511octets|pkts512to1023octets|pkts1024to1518octets) <1-2147483647> (absolute|delta) rising <0-2147483647> <0-65535> falling <0-2147483647> <0-65535> startup (rising|rising-falling|falling) [owner NAME]
	no rmon alarm <1-65535>
Parameter	**<1-65535>**:Specify to index of alarm
	interface IF_PORT:specifies port list to set
	<1-2147483647>:sample interval
	<0-2147483647>:threshold of rising
	<0-65535> :event index of rising
	<0-2147483647>:threshold of falling
	<0-65535>:event index of falling
Default	
Mode	Global configuration

Usage	Use the **rmon alarm interface broadcast-pkts absolute rising falling startup falling** command to set configuration rmon event. Use the **no** form of this command to restore to default setting.

Example:

The following example specifies that set configuration rmon event test.

```
Switch(config)# rmon alarm 1 interface gi1 broadcast-pkts 1 absolute rising
10 1 falling 1 2 startup falling
Falling Event is not exist.Input Parameter Error
```

32.6. rmon history

Item	Description
Syntax	rmon history <1-65535> interface IF_PORT [buckets <1-50>] [interval <1-3600>] [owner NAME]
	no rmon history <1-65535>
Parameter	**<1-65535>**:Specify to index of history
	interface IF_PORT:specifies port list to set
	<1-50>:the maximum number of buckets value
	<1-3600>:the number of seconds value.
	NAME :
Default	
Mode	Global configuration
Usage	Use the **rmon history interface buckets interval owner** command to set configuration rmon event. Use the **no** form of this command to restore to default setting.

Example:

The following example specifies that set configuration rmon event test.

```
Switch(config)# rmon history 1 interface gi1 buckets 1 interval  2 owner
test
```

33. gvrp

33.1. gvrp

Item	Description
Syntax	gvrp no gvrp
Parameter	
Default	
Mode	Global Configuration
Usage	Use the **gvrp** command to set gvrp state. Use the **no** form of this command to default setting. You can verify your setting by entering the show gvrp Privileged EXEC command.

Example:

The following example specifies that set gvrp test.

```
Switch(config)# gvrp
```

33.2. show gvrp

Item	Description
Syntax	show gvrp
Parameter	
Default	
Mode	Privileged EXEC
Usage	Use the command **show gvrp** in the Privileged EXEC mode.

Example:

The following example shows the gvrp status.

```
Switch# show gvrp
                GVRP    Status
                --------------------
    GVRP                          : Disabled
    Join time                     : 200 ms
    Leave time                    : 600 ms
    LeaveAll time                 : 10000 ms
```

33.3. gvrp statistics

Item	Description
Syntax	show gvrp statistics [interfaces IF_PORTS]
	clear gvrp statistics [interfaces IF_PORTS]
Parameter	**interfaces IF_PORTS**:Specify the ports to display information
Default	
Mode	Privileged EXEC
Usage	Use the command **show gvrp statistics** in the Privileged EXEC mode. Use the **clear clear gvrp statistics** command to clear statistics that are recorded on interface.

Example:

The following example shows the gvrp statistics information.

```
Switch# show gvrp statistics interfaces gi1
Port id         :  gi1
Total RX        :    0
JoinEmpty RX    :    0
JoinIn RX       :    0
Empty RX        :    0
LeaveIn RX      :    0
LeaveEmpty RX   :    0
LeaveAll RX     :    0
Total TX        :    0
JoinEmpty TX    :    0
JoinIn TX       :    0
Empty TX        :    0
LeaveIn TX      :    0
LeaveEmpty TX   :    0
LeaveAll TX     :    0
```

33.4. gvrp error-statistics

Item	Description
Syntax	show gvrp error-statistics [interfaces IF_PORTS]
	clear gvrp error-statistics [interfaces IF_PORTS]
Parameter	**interfaces IF_PORTS**:Specify the ports to display information
Default	
Mode	Privileged EXEC
Usage	Use the command **show gvrp error-statistics** in the Privileged EXEC mode.

	Use the **clear gvrp error-statistics** command to clear error statistics that are recorded on interface.

Example:

The following example shows the gvrp error-statistics information.

```
Switch# show gvrp error-statistics interfaces gi1
Legend:
INVPROT : Invalid protocoal Id
INVATYP : Invalid Attribute Type   INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value  INVEVENT: Invalid Event
  Port   | INVPROT | INVATYP | INVALEN | INVAVAL | INVEVENT
   gi1           0         0         0         0         0
```

33.5. show gvrp configuration

Item	Description
Syntax	show gvrp configuration [interfaces IF_PORTS]
Parameter	**interfaces IF_PORTS**:Specify the ports to display information
Default	
Mode	Privileged EXEC
Usage	Use the command **show gvrp configuration** in the Privileged EXEC mode.

Example:

The following example shows the gvrp configuration information.

```
Switch# show gvrp configuration interfaces gi1
  Port   |  GVRP-Status   | Registration   | Dynamic VLAN Creation
--------+---------------+---------------+----------------------
 gi1           Disabled          Normal             Enabled
```

33.6. gvrp registration-mode

Item	Description
Syntax	gvrp registration-mode (normal|fixed|forbidden)
Parameter	**normal**:Normal mode
	fixed:Fixed mode
	forbidden:Forbidden mode
Default	Default is normal mode
Mode	Interface Configuration
Usage	Use the **gvrp registration-mode** command to set gvrp registration-mode.

Example:

The following example specifies that set gvrp registration-mode test.

```
Switch(config-if)# gvrp registration-mode fixed
```

33.7. gvrp vlan-creation-forbid

Item	Description
Syntax	gvrp vlan-creation-forbid
	no gvrp vlan-creation-forbid
Parameter	
Default	
Mode	Interface Configuration
Usage	Use the **gvrp vlan-creation-forbid** command to set VLAN creation state. Use the **no** form of this command to default setting.

Example:

The following example specifies that set gvrp VLAN creation state test.

```
Switch(config-if)# gvrp vlan-creation-forbid
```