

**FiberstoreOS**

**Network Management Command Line Reference**

# Contents

---

<b>1 Network Diagnosis Commands.....</b>	<b>5</b>
1.1 ping.....	5
1.2 traceroute.....	6
<b>2 NTP Commands.....</b>	<b>8</b>
2.1 ntp ace.....	8
2.2 ntp authentication.....	9
2.3 ntp broadcast client.....	10
2.4 ntp broadcastdelay.....	11
2.5 ntp disable.....	12
2.6 ntp key.....	13
2.7 ntp interface reload.....	13
2.8 ntp peer.....	14
2.9 ntp refclock.....	15
2.10 ntp server.....	16
2.11 ntp trustedkey.....	17
2.12 show ntp.....	18
2.13 show ntp ace.....	19
2.14 show ntp associations.....	20
2.15 show ntp key.....	21
2.16 show ntp status.....	22
2.17 show ntp statistics.....	23
2.18 clear ntp statistics.....	24
<b>3 Phy Loopback Commands.....</b>	<b>25</b>
3.1 loopback phy.....	25
3.2 loopback port.....	26
3.3 no loopback.....	27
3.4 show phy loopback.....	27
3.5 l2 ping.....	28
3.6 l2 ping response.....	29
3.7 show l2ping response.....	30
3.8 debug l2ping.....	31
3.9 show debugging l2ping.....	32
<b>4 RMON1 Commands.....</b>	<b>33</b>
4.1 rmon collection stats.....	33
4.2 rmon collection history.....	34

---

4.3 rmon event.....	35
4.4 rmon alarm.....	36
4.5 show rmon statistics.....	37
4.6 show rmon history.....	38
4.7 show rmon event.....	39
4.8 show rmon alarm.....	40
4.9 rmon clear counters.....	41
4.10 debug rmon.....	42
<b>5 SNMP Commands.....</b>	<b>43</b>
5.1 snmp-server access.....	43
5.2 snmp-server community.....	44
5.3 snmp-server context.....	45
5.4 snmp-server enable.....	46
5.5 snmp-server engineID.....	47
5.6 snmp-server group.....	48
5.7 snmp-server notify.....	49
5.8 snmp-server system-contact.....	50
5.9 snmp-server system-location.....	50
5.10 snmp-server target-address.....	51
5.11 snmp-server trap enable.....	53
5.12 snmp-server trap delay.....	54
5.13 snmp-server trap target-address.....	54
5.14 snmp-server inform target-address.....	56
5.15 snmp-server usm-user.....	57
5.16 snmp-server target-params.....	58
5.17 snmp-server version.....	59
5.18 snmp-server view.....	60
5.19 snmp-server access-group NAME in.....	61
5.20 show snmp.....	62
5.21 show snmp-server access.....	63
5.22 show snmp-server community.....	64
5.23 show snmp-server context.....	64
5.24 show snmp-server engineID.....	65
5.25 show snmp-server group.....	66
5.26 show snmp-server notify.....	67
5.27 show snmp-server sys-info.....	68
5.28 show snmp-server trap-receiver.....	68
5.29 show snmp-server usm-user.....	69
5.30 show snmp-server version.....	70
5.31 show snmp-server view.....	71
<b>6 SFLOW Commands.....</b>	<b>73</b>
6.1 sflow enable.....	73
6.2 sflow collector.....	73

---

6.3 sflow counter interval.....	74
6.4 sflow counter enable.....	75
6.5 sflow sample rate.....	76
6.6 sflow sample enable.....	77
6.7 show sflow.....	78
<b>7 LLDP Commands.....</b>	<b>80</b>
7.1 lldp enable(global).....	80
7.2 lldp enable(interface).....	80
7.3 lldp system-name.....	81
7.4 lldp system-description.....	82
7.5 lldp management ip.....	83
7.6 lldp msg-tx-hold.....	84
7.7 lldp timer msg-tx-interval.....	85
7.8 lldp timer reinit-delay.....	86
7.9 lldp timer tx-delay.....	87
7.10 lldp tlv basic.....	87
7.11 lldp tlv 8021-org-specific.....	89
7.12 lldp tlv 8023-org-specific.....	90
7.13 lldp tlv med.....	91
7.14 debug lldp.....	92
7.15 show lldp local.....	93
7.16 show lldp neighbor.....	94
7.17 show lldp statistics.....	95
7.18 clear lldp statistics.....	96

---

# 1 Network Diagnosis Commands

---

## 1.1 ping

The switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response- The normal response (hostname is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond- If the host does not respond, a no-answer message is returned.
- Unknown host- If the host does not exist, an unknown host message is returned.
- Destination unreachable- If the default gateway cannot reach the specified network, a destination-unreachable message is returned.
- Network or host unreachable- If there is no entry in the route table for the host or network, a network or host unreachable message is return.

### Command Syntax

**ping** (ip|vrf *WORD* |mgmt-if) *WORD*

**ping** ipv6 *WORD* (interface *IFNAME* |)

**ping** mgmt-if ipv6 *WORD*

**ping**

<b>ip</b>	Public network IPv4 echo
<b>vrf</b> <i>WORD</i>	VPN Routing/Forwarding instance
<b>mgmt-if</b>	Management interface
<b>mpls</b>	MPLS LSP ping
<i>WORD</i>	Ping destination IPv4 or IPv6 address or hostname
<b>ipv6</b>	Public network IPv6 echo
<b>interface</b>	Outgoing interface for LinkLocal address/host

<i>IFNAME</i>	Interface's name
---------------	------------------

## Command Mode

Privileged EXEC

## Default

None

## Usage

None

## Examples

This example shows how to ping a host from management interface.

```
Switch# ping mgmt-if 10.10.29.247
```

```
PING 10.10.29.247 (10.10.29.247) 56(84) bytes of data:
64 bytes from 10.10.29.247: icmp_seq=1 ttl=64 time=0.194 ms
64 bytes from 10.10.29.247: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 10.10.29.247: icmp_seq=3 ttl=64 time=0.134 ms
64 bytes from 10.10.29.247: icmp_seq=4 ttl=64 time=0.121 ms
64 bytes from 10.10.29.247: icmp_seq=5 ttl=64 time=0.135 ms

--- 10.10.29.247 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.121/0.143/0.194/0.025 ms
```

## Related Commands

**traceroute**

## 1.2 traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your switches can participate as the source or destination of the traceroute privileged EXEC command and might or might not appear as a hop in the traceroute command output. If the switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output.

Intermediate switches do not show up in the traceroute output if they are only bridging the packet

from one port to another within the same VLAN. However, if the intermediate switch is a multilayer switch that is routing a particular packet, this switch shows up as a hop in the traceroute output.

The traceroute privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute determines the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

## Command Syntax

**traceroute** (**ip|ipv6**| **vrf** *WORD* |**mgmt-if**) (*WORD*)

<b>ip</b>	Public network IPv4 echo
<b>ipv6</b>	Public network IPv6 echo
<b>vrf</b>	VPN Routing/Forwarding instance
<b>mgmt-if</b>	Management interface
<i>WORD</i>	Destination IP address or hostname

## Command Mode

Privileged EXEC

## Default

None

## Usage

None

## Examples

The following example is sample dialog from the traceroute command using default values.

```
Switch# traceroute 1.1.1.2
```

```
traceroute to 1.1.1.2 (1.1.1.2), 30 hops max, 38 byte packets
 1  1.1.1.2 (1.1.1.2)  108.129 ms  99.313 ms  94.720 ms
```

## Related Commands

**ping**

## 2 NTP Commands

### 2.1 ntp ace

To create the Access Control Entries (ACE) of a NTP server/peer, use the `ntp ace` command in global configuration mode. To remove the ace, use the `no` form of this command.

#### Command Syntax

```
ntp ace (address | hostname) (mask LEN) {version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited}
```

```
ntp ace (address | hostname) (mask LEN) none
```

```
no ntp ace (address | hostname) (mask LEN) {version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited }
```

```
no ntp ace (address | hostname) (mask LEN)
```

<i>address</i>	IPv4 or IPv6 address of the time server or peer
<i>hostname</i>	Name of the time server or peer
<b>mask</b> <i>LEN</i>	Specify network mask of the address
<b>version</b>	Ignore these hosts if not the current NTP version
<b>kod</b>	If access is denied, send a kiss-of-death packet
<b>ignore</b>	Ignore all packets from host that match this entry
<b>noquery</b>	Ignore all NTP mode 6 and 7 packets from the source, time service is not affected
<b>nomodify</b>	Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server
<b>notrap</b>	Decline to provide mode 6 control message trap service to matching hosts
<b>noserve</b>	Ignore NTP packets whose mode is other than 6 or 7
<b>nopeer</b>	Provide stateless time service to polling hosts, but do not allocate peer memory resources



<b>notrust</b>	Treat these hosts normally in other respects, but never use them as synchronization sources
<b>limited</b>	These hosts are subject to limitation of number of clients from the same net
<b>none</b>	No limit

## Command Mode

Global Configuration

## Default

None

## Usage

Use this command if you want to allow the system to synchronize with the specified server. The server will not synchronize to this machine.

## Examples

The following example shows how to create an ACE for 1.1.1.1:

```
Switch# configure terminal
```

```
Switch(config)# ntp ace 1.1.1.1 version
```

## Related Commands

**show ntp**

## 2.2 ntp authentication

To enable NTP authentication, use the `ntp authentication enable` command. To disable the NTP authentication, use the `ntp authentication disable` command.

## Command Syntax

**ntp authentication (enable | disable)**

<b>enable</b>	Enable NTP authentication
<b>disable</b>	Disable NTP authentication

## Command Mode

Global Configuration

## Default

None

## Usage

When NTP authentication is enabled, the switch will synchronize the time with NTP servers with trusted key only. For more information about trusted key, please see the `ntp trustedkey` command.

## Examples

The following example shows how to enable NTP authentication:

```
Switch# configure terminal
```

```
Switch(config)# ntp authentication enable
```

## Related Commands

**show ntp**

## 2.3 ntp broadcast client

To configure the system to receive Network Time Protocol (NTP) broadcast packets on a specified interface, use the `ntp broadcast client` command in interface configuration mode. To disable this capability, use the `no` form of this command.

## Command Syntax

**ntp broadcast client**

**no ntp broadcast client**

## Command Mode

Interface Configuration

## Default

None

## Usage

Use this command to allow the system to listen to broadcast packets on an interface-by-interface.

## Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface eth-0-1:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# ntp broadcast client
```

## Related Commands

**ntp broadcastdelay**

## 2.4 ntp broadcastdelay

To configure the change the estimated round-trip delay between the switch and the NTP broadcast server, use the `ntp broadcastdelay` command in global configuration mode. To disable this capability, use the `no` form of this command.

## Command Syntax

**ntp broadcastdelay** *delay*

**no ntp broadcastdelay**

<i>delay</i>	Delayed time interval in milliseconds, the range is 1-10000
--------------	-------------------------------------------------------------

## Command Mode

Global Configuration

## Default

None

## Usage

The default value should be 3000 milli-seconds.

## Examples

The following example shows how to change broadcast delay to 2000ms:

```
Switch# configure terminal
```

```
Switch(config-if)# ntp broadcastdelay 2000
```

## Related Commands

**ntp broadcast client**

## 2.5 ntp disable

To configure Disable NTP packets from being received on the interface, use the `ntp disable` command in interface configuration mode. To disable this capability, use the `no` form of this command.

## Command Syntax

**ntp disable**

**no ntp disable**

## Command Mode

Interface Configuration

## Default

By default, all interfaces receive NTP packets.

## Usage

None

## Examples

In the following example, the system is configured not to received NTP packet in interface eth-0-1:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# ntp disable
```

## Related Commands

None

## 2.6 ntp key

To configure value of the NTP key, use the `ntp key` command in global configuration mode. To remove the value of the NTP key, use the `no` form of this command.

### Command Syntax

**ntp key** *keyid value*

**no ntp key** *keyid*

<i>keyid</i>	Authentication key (1 to 64000)
<i>value</i>	The value of the key

### Command Mode

Global Configuration

### Default

None

### Usage

Use this command to create a value for a NTP key.

### Examples

In the following example, the value 321 is given to the NTP key 123:

```
Switch# configure terminal
```

```
Switch(config)# ntp key 123 321
```

### Related Commands

**show ntp key**

## 2.7 ntp interface reload

To reload the NTP configuration on the interfaces, use the `ntp interface reload` command in global configuration mode.

## Command Syntax

**ntp interface reload**

## Command Mode

Global Configuration

## Default

None

## Usage

Use this command to reload the NTP configuration on all the interfaces.

## Examples

The following example reloads the NTP configuration on all interfaces:

```
Switch# configure terminal
```

```
Switch(config)# ntp interface reload
```

## Related Commands

**show ntp**

## 2.8 ntp peer

To configure the software clock to synchronize a peer or to be synchronized by a peer, use the `ntp peer` command in global configuration mode. To disable this capability, use the `no` form of this command.

### Command Syntax

**ntp peer** ( *hostname* | *address* ) { **key** *key-id* | **prefer** | **version** *number* }

**no ntp peer** ( *hostname* | *address* )

<i>hostname</i>	Name of the time server or peer
<i>address</i>	IPv4 or IPv6 address of the time server or peer
<b>key</b> <i>key-id</i>	Authentication key to use when sending packets to this peer (1 to 64000)
<b>prefer</b>	Makes this peer the preferred peer that provides synchronization

<b>version number</b>	Defines the Network Time Protocol (NTP) version number
-----------------------	--------------------------------------------------------

## Command Mode

Global Configuration

## Default

None

## Usage

When a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Use this command to allow a device to synchronize with a peer, or vice versa. Using the `prefer` keyword reduces switching between peers.

## Examples

The following example shows how to configure a switch to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IP address 192.168.22.33 using NTP version 2.

```
Switch# configure terminal
```

```
Switch(config)# ntp peer 192.168.22.33 version 2
```

## Related Commands

**show ntp**

## 2.9 ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the `ntp refclock` command in global configuration mode. To disable support of the external time source, use the `no` form of this command.

## Command Syntax

**ntp refclock stratum *number***

**no ntp refclock**

<i>number</i>	Number from 1 to 15. Indicates the NTP stratum number that the system will claim.
---------------	-----------------------------------------------------------------------------------

## Command Mode

Global Configuration

## Default

This command is disabled by default.

## Usage

None

## Examples

The following example shows configuration of a NTP source on a switch platform:

```
Switch# configure terminal
```

```
Switch(config)# ntp refclock stratum 1
```

## Related Commands

**show ntp**

## 2.10 ntp server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the `ntp server` command in global configuration mode. To disable this capability, use the `no` form of this command.

## Command Syntax

```
ntp server ( hostname | address ) {key key-id | prefer| version number}
```

```
no ntp server ( hostname | address )
```

<i>hostname</i>	Name of the time server or peer
<i>address</i>	IPv4 or IPv6 address of the time server or peer
<b>key</b> <i>key-id</i>	Authentication key to use when sending packets to this peer (1 to 64000)



<b>prefer</b>	Makes this peer the preferred peer that provides synchronization
<b>version number</b>	Defines the Network Time Protocol (NTP) version number

## Command Mode

Global Configuration

## Default

The server will not synchronize to this machine.

## Usage

Use this command if you want to allow the system to synchronize with the specified server.

## Examples

The following example shows how to configure a switch to allow its software clock to be synchronized with the clock by the device at IP address 172.16.22.44 using NTP version 2:

```
Switch# configure terminal
```

```
Switch(config)# ntp server 172.16.22.44 version 2
```

## Related Commands

**show ntp**

## 2.11 ntp trustedkey

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the `ntp trustedkey` command in global configuration mode. To disable authentication of the identity of the system, use the `no` form of this command.

## Command Syntax

**ntp trustedkey** *key-id*

**no ntp trustedkey** *key-id*

<i>key-id</i>	Authentication key to use when sending packets to this peer (1 to 64000)
---------------	--------------------------------------------------------------------------

## Command Mode

Global Configuration

## Default

None

## Usage

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the `ntp key` command) that a peer NTP system must provide in its NTP packets, in order for this system to synchronize to it. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

## Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Switch# configure terminal
Switch(config)# ntp authentication enable
Switch(config)# ntp key 42 aNiceKey
Switch(config)# ntp trustedkey 42
```

## Related Commands

`show ntp`  
`ntp key`

## 2.12 show ntp

To display the NTP configurations, use the `show ntp` command in privileged EXEC mode.

## Command Syntax

`show ntp`

## Command Mode

Privileged EXEC

## Default

None

## Usage

Use this command to display the NTP configurations.

## Examples

The following example shows the configuration of NTP:

```
Switch# show ntp
```

```
Current NTP configuration:
```

```
=====
```

```
NTP access control list:
```

```
Unicast peer:
```

```
 1.1.1.1
```

```
Unicast server:
```

```
 2.2.2.2
```

```
Broadcast client: enabled
```

```
Authentication: enabled
```

```
Local reference clock:
```

```
enabled, stratum 10
```

## Related Commands

**ntp server**

**ntp peer**

## 2.13 show ntp ace

To display the restrict list of Access Control Entries (ACE) of a NTP server/peer, use the `show ntp ace` command in privileged EXEC mode.

## Command Syntax

**show ntp ace**

## Command Mode

Privileged EXEC

## Default

None

## Usage

None.

## Examples

The following example shows the NTP restrict list:

```
Switch# show ntp ace
```

address	mask	count	flags
0.0.0.0	0.0.0.0	55188	noquery, nomodify, notrap
6.6.6.6	255.255.255.255	73	none
127.0.0.1	255.255.255.255	1259	none

## Related Commands

**ntp ace**

## 2.14 show ntp associations

To show the status of Network Time Protocol (NTP) associations, use the `show ntp associations` command in privileged EXEC mode.

## Command Syntax

**show ntp associations**

## Command Mode

Privileged EXEC

## Default

None

## Usage

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

## Examples

The following example shows the status of NTP associations:

```
Switch# show ntp associations
```

```
Current NTP associations:
```

```
remote      refid      st when poll reach  delay  offset disp
=====
*6.6.6.6    127.127.1.0  6 161 256 377  0.778 -0.087 119.400
* synchronized, + candidate, # selected, x falsetick, . excess, - outlier
```

## Related Commands

**show ntp status**

## 2.15 show ntp key

To show the NTP keys, use the show ntp key command in privileged EXEC mode.

### Command Syntax

**show ntp key**

### Command Mode

Privileged EXEC

### Default

None

### Usage

Use this command to display the NTP keys.

### Examples

The following example shows the keys of NTP:

Switch# show ntp key

```
Current NTP key configuration:
=====
 1 abcd
64000 KKKK
```

## Related Commands

**ntp key**

## 2.16 show ntp status

To show the status of the Network Time Protocol (NTP), use the `show ntp status` command in privileged EXEC mode.

### Command Syntax

**show ntp status**

### Command Mode

Privileged EXEC

### Default

None

### Usage

None.

### Examples

The following is sample output from the `show ntp status` command:

Switch# show ntp status

```
Current NTP status:
=====
clock is synchronized
stratum:          11
reference clock:  127.127.1.0
frequency:        0.000 ppm
precision:        2**15
reference time:   d116c946.4dc2f6a7 ( 1:24:22.303 UTC Tue Mar 1 2011)
root delay:       0.000 ms
root dispersion:  449.207 ms
peer dispersion:  662.059 ms
clock offset:     0.000 ms
stability:        0.000 ppm
```

### Related Commands

**show ntp associations**

## 2.17 show ntp statistics

To show the statistics of the Network Time Protocol (NTP), use the `show ntp statistics` command in privileged EXEC mode.

### Command Syntax

`show ntp statistics`

### Command Mode

Privileged EXEC

### Default

None

### Usage

None.

### Examples

The following is sample output from the `show ntp statistics` command:

Switch# show ntp statistics

```
Current NTP I/O statistics:
=====
time since reset: 175834
receive buffers: 10
free receive buffers: 9
used receive buffers: 0
low water refills: 1
dropped packets: 0
ignored packets: 0
received packets: 32
packets sent: 31
packets not sent: 0
interrupts handled: 32
received by int: 32
```

### Related Commands

`show ntp associations`

## 2.18 clear ntp statistics

To clear the statistics of the Network Time Protocol (NTP), use the `clear ntp statistics` command in privileged EXEC mode.

### Command Syntax

`clear ntp statistics`

### Command Mode

Privileged EXEC

### Default

None

### Usage

None.

### Examples

The following is sample that clear ntp statistics:

```
Switch# clear ntp statistics
```

### Related Commands

`show ntp statistics`



## 3 Phy Loopback Commands

---

### 3.1 loopback phy

Use this command to configure a physical interface as phy level loopback mode. Use the no loopback command to cancel this configuration.

#### Command Syntax

**loopback phy** (**internal** *IFPHYSICAL* | **external**)

<b>internal</b> <i>IFPHYSICAL</i>	Packets transmitted to the interface should be looped back to a specified physical interface without any modification. The destination physical interface
<b>external</b>	Packets received from the interface should be looped back to the interface itself without any modification

#### Command Mode

Interface Configuration

#### Defaults

No loopback.

#### Usage

Only one type of loopback can be applied on a physical interface. A new configuration should replace the old configuration.

#### Examples

In the following example, the physical interface is set to phy level loopback mode:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# loopback phy internal eth-0-2
```

## Related Commands

**no loopback**

## 3.2 loopback port

Use this command to configure a physical interface as port level loopback mode. Use the no loopback command to cancel this configuration.

### Command Syntax

**loopback port (mac-address swap)**

<b>mac-address swap</b>	If this field is entered, the packet's SMAC incoming from port level loopback interface will be swapped with its DMAC, and the FCS will be updated
-------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

### Command Mode

Interface Configuration

### Defaults

No mac-address swap.

### Usage

Only one type of loopback can be applied on a physical interface. A new configuration should replace the old configuration.

### Examples

In the following example, the physical interface is set to port level loopback mode:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# loopback port
```

### Related Commands

**no loopback**

## 3.3 no loopback

Use this command to cancel a physical interface from phy level or port level loopback to normal interface.

### Command Syntax

**no loopback**

### Command Mode

Interface Configuration

### Defaults

This command has no default settings.

### Usage

Phy or port level loopback can be canceled by this command.

### Examples

In the following example, port level loopback is canceled by this command:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# loopback port
```

```
Switch(config-if)# no loopback
```

### Related Commands

**phy loopback**

**port loopback**

## 3.4 show phy loopback

Use this command to show the configuration of phy loopback.

### Command Syntax

**show phy loopback**

## Command Mode

Privileged EXEC

## Defaults

This command has no default settings.

## Usage

None

## Examples

In the following example shows how to show the configuration:

Switch# show phy loopback

Interface	Type	DestIntf	SwapMac
eth-0-1	port	-	no
eth-0-2	port	-	yes
eth-0-3	external	-	-
eth-0-4	internal	eth-0-5	-

## Related Commands

**phy loopback**

**port loopback**

## 3.5 l2 ping

Use this command to ping specified DMAC from specified physical interface, using protocol packet with ethertype 0x9009. Use the l2 ping stop command to stop the ping when l2 ping is started.

## Command Syntax

**l2 ping** *HHHH.HHHH.HHHH* **interface** *IFPHYSICAL* (**{vlan** <1-4094> **|interval** <1-65535> **|**  
**timeout** <1-65535> **|count** <1-65535> **|size** <64-1518>} |)

<i>HHHH.HHHH.HHHH</i>	The DMAC to ping
<i>IFPHYSICAL</i>	The interface to ping from
<b>vlan</b> <1-4094>	The vlan id of the protocol ping packet

<b>interval</b> <1-65535>	The interval time between two ping action, millisecond
<b>timeout</b> <1-65535>	The time wait for a ping action, millisecond
<b>count</b> <1-65535>	Total ping times
<b>size</b> <64-1518>	The size of the protocol ping packe

## Command Mode

Privileged EXEC

## Defaults

The ping protocol packet is without vlan tag by default.

The default interval ping time is 5 seconds.

The default count is 5.

The default size of the ping protocol packet is 64.

## Usage

The ping action can be canceled by “Ctrl + C”.

## Examples

The following example shows how to ping a specified destination mac.

```
Switch# 12 ping 0000.0000.0001 interface eth-0-1 vlan 101 interval 200 timeout 1000 count 10 size 1500
```

## Related Commands

**12 ping response**

## 3.6 12 ping response

Use this command to enable 12 ping response globally. Use the no form of this command to disable it.

## Command Syntax

**12 ping response enable**

**no 12 ping response enable**

## Command Mode

Interface Configuration

## Defaults

This command has no default settings.

## Usage

If l2 ping response is not enabled, the l2 ping request packet should be dropped.

## Examples

In the following example shows how to enable l2 ping response on interface:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# l2 ping response enable
```

## Related Commands

**l2 ping**

**show l2ping response**

## 3.7 show l2ping response

Use this command to show the configuration of l2 ping.

## Command Syntax

**show l2ping response**

## Command Mode

Privileged EXEC

## Defaults

This command has no default settings.

## Usage

None

## Examples

In the following example shows how to use this command:

Switch# show l2 ping response

```
Interface      L2pingResp
-----
eth-0-7        Enable
eth-0-8        Enable
-----
```

## Related Commands

**l2 ping response**

## 3.8 debug l2ping

Use this command to enable debugging l2 ping.

### Command Syntax

**debug l2ping** (all | packet | send | receive| response)

**no debug l2ping** (all | packet | send | receive|response)

<b>all</b>	All packet
<b>packet</b>	Packet
<b>send</b>	Send packets
<b>receive</b>	Receive packets
<b>response</b>	Response

### Command Mode

Privileged EXEC

### Defaults

All these three debugging types is off.

### Usage

If packet, send, or receive debugging is on, the corresponding message will be printed.

## Examples

In the following example shows how to use this command:

```
Switch# debug l2ping all
```

## Related Commands

**l2 ping response**

## 3.9 show debugging l2ping

Use this command to show the status of l2ping debugging

### Command Syntax

```
show debugging l2ping
```

### Command Mode

Privileged EXEC

### Defaults

This command has no default settings.

### Usage

none

## Examples

In the following example shows the status of l2ping debuggin:

```
Switch# show debugging l2ping
```

```
L2ping debugging status:  
l2ping packet debugging is on  
l2ping receive debugging is on  
l2ping send debugging is on
```

## Related Commands

**l2 ping response**



# 4 RMON1 Commands

---

## 4.1 rmon collection stats

Use this command to enable RMON statistic collection on the interface

### Command Syntax

**rmon collection stats** *ID* (**owner** *WORD*| )

**no rmon collection stats** *ID*

<i>ID</i>	Specify the RMON group of statistics. The range is 1~65535
<b>owner</b> <i>WORD</i>	The owner identity of the statistic.(optional)

### Command Mode

Interface Configuration

### Default

None

### Usage

To create one statistic only on a certain interface

### Examples

This example shows how to collect RMON statistics for the owner test

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# rmon collection stats 1 owner test
```

## Related Commands

**show rmon statistics**

## 4.2 rmon collection history

Use this command to enable RMON history collection for the specified number of buckets and time period

### Command Syntax

**rmon collection history** *Index* (**buckets** *numbs*) (**interval** *values*) (**owner** *WORD*)

**no rmon collection history** *Index*

<i>Index</i>	Specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1~65535
<b>buckets</b> <i>numbs</i>	Specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1~65535
<b>interval</b> <i>values</i>	Specify the number of seconds in each polling cycle. The range is 1~3600
<b>owner</b> <i>WORD</i>	The owner identity of history group (optional)

### Command Mode

Interface Configuration

### Default

None

### Usage

Use this command to enable a history statistics on a certain interface.

### Examples

This example shows how to enable history RMON statistics on eth-0-1

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# rmon collection history 1 buckets 1000 interval 100 owner test
```

## Related Commands

**show rmon history**

## 4.3 rmon event

Use this command to add a event to RMON event table

### Command Syntax

**rmon event** *Index* (**log** |)(**trap** *WORD* |) (**description** *WORD*) (**owner** *WORD*)

**no rmon event** *Index*

<i>Index</i>	Event index. The range is 1~65535
<b>log</b>	Generate a RMON log when event is triggered
<b>trap</b> <i>WORD</i>	Trap community
<b>description</b> <i>WORD</i>	Specify the description string for the event (default is RMON_SNMP)
<b>owner</b> <i>WORD</i>	The owner name (default is RMON_SNMP)

### Command Mode

Global Configuration

### Default

None

### Usage

Create a event is for RMON alarm. Permit event special traiggered operate. Log can be sent by trap.

### Examples

This example shows how to create a event

Switch# configure terminal

Switch(config)# rmon event 1 log trap public description reach\_max owner test

### Related Commands

**show rmon event**

## 4.4 rmon alarm

Use this command to set a alarm on a MIB object.

### Command Syntax

**rmon alarm** *Index* (*WORD*) **interval** *values* (**delta** | **absolute**) **rising-threshold** *holds*( **event numbs**|)  
**falling-threshold** *holds*( **event numbs**|) (**owner** *WORD*| )

**no rmon alarm** *Index*

<i>Index</i>	Alarm index. The range is 1~65535
<i>WORD</i>	Variable for setting alarm(etherStatsEntry.m.n)
<b>interval</b> <i>values</i>	Specify the time in seconds the alarm monitors the MIB object(seconds). The range is 1~65535
<b>delta</b>	Specify the delta keyword to test the change between samples of a MIB variable
<b>absolute</b>	Specify the absolute keyword to test each MIB variable directly
<b>rising-threshold</b> <i>holds</i>	Alarm rising threshold. <-2147483648-2147483646>
<b>event numbs</b>	Specify the event number to trigger when the rising threshold exceeds its limit
<b>falling-threshold</b> <i>holds</i>	Alarm falling threshold. <-2147483648-2147483646>
<b>event numbs</b>	Specify the event number to trigger when the falling threshold exceeds its limit. The range is 1~65535
<b>owner</b> <i>WORD</i>	The owner identity of the alarm

### Command Mode

Global Configuration

### Default

None

### Usage

We need to create events for rising threshold and falling threshold first before we create a alarm for a mib.

Also the statistics need to be created on a interface, because we only support to set alarm monitor on etherStatsEntry.

## Examples

This example shows how to set a alarm

```
Switch# configure terminal
```

```
Switch(config)# rmon alarm 1 etherStatsEntry.3.1 interval 10 delta rising-threshold 1000 event 1  
falling-threshold 5 event 1 owner test
```

## Related Commands

None

## 4.5 show rmon statistics

Use this command to show rmon statistics.

### Command Syntax

```
show rmon statistics (statistics_id |)
```

<i>statistics_id</i>	Statistics index. <1-65535>
----------------------	-----------------------------

### Command Mode

Privileged EXEC

### Default

None

### Usage

Show the interface statistics which collect by RMON

## Examples

This example shows how to show rmon statistics

```
Switch# show rmon statistics
```

```
Rmon collection index 1
```

```
Statistics ifindex = 1, Owner: RMON_SNMP
Input packets 0, octets 0, dropped 0
Broadcast packets 0, multicast packets 0, CRC alignment errors 0, collisions 0
Undersized packets 0, oversized packets 0, fragments 0, jabbers 0
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0
256-511: 0, 512-1023: 0, 1024-max: 0
```

## Related Commands

None

## 4.6 show rmon history

Use this command to show rmon history statistics.

### Command Syntax

**show rmon history** (*history\_id* |)

<i>history_id</i>	History index. The range is 1~65535
-------------------	-------------------------------------

### Command Mode

Privileged EXEC

### Default

None

### Usage

Show the interface history statistics which collect by RMON

### Examples

This example shows how to show rmon history statistics

Switch# show rmon history

```
History index = 1
Data source ifindex = 1
Buckets requested = 1000
Buckets granted = 1000
Interval = 100
Owner: test
```

```
Sample # 1 Begin at 00:30:07
Received 00 octets, 00 packets
00 broadcast and 00 multicast packets
00 undersized and 00 oversized packets
00 fragments and 00 jabbers
00 CRC alignment errors and 00 collisions.
# of dropped packet events is 00
Network utilization is estimated at 0
Sample # 2 Begin at 00:31:47
Received 00 octets, 00 packets
00 broadcast and 00 multicast packets
00 undersized and 00 oversized packets
00 fragments and 00 jabbers
00 CRC alignment errors and 00 collisions.
# of dropped packet events is 00
Network utilization is estimated at 0
Sample # 3 Begin at 00:33:27
Received 00 octets, 00 packets
00 broadcast and 00 multicast packets
00 undersized and 00 oversized packets
00 fragments and 00 jabbers
00 CRC alignment errors and 00 collisions.
# of dropped packet events is 00
Network utilization is estimated at 0
```

## Related Commands

None

## 4.7 show rmon event

Use this command to show rmon event.

### Command Syntax

```
show rmon event (event_id |)
```

<i>event_id</i>	Event index. The range is 1~65535
-----------------	-----------------------------------

### Command Mode

Privileged EXEC

### Default

None

## Usage

Show rmon events information

## Examples

This example shows how to show rmon event

Switch# show rmon event

```
event Index = 1
  Description: RMON_SNMP
  Event type Log & Trap
  Event community name public
  Last Time Sent = 00:00:00
  Owner test
```

## Related Commands

None

## 4.8 show rmon alarm

Use this command to show rmon alarm

## Command Syntax

**show rmon alarm** (*alarm\_id* |)

<i>alarm_id</i>	Alarm index. The range is 1~65535
-----------------	-----------------------------------

## Command Mode

Privileged EXEC

## Default

None

## Usage

Show rmon alarm information

## Examples

This example shows how to show rmon alarm



Switch#show rmon alarm

```
alarm Index = 1
alarm status = VALID
    alarm Interval = 3600
    alarm Type is Delta
    alarm Value = 00
    alarm Rising Threshold = 100
    alarm Rising Event = 1
    alarm Falling Threshold = 10
    alarm Falling Event = 1
    alarm Owner is test
```

## Related Commands

None

## 4.9 rmon clear counters

Use this command to clear rmon counters.

### Command Syntax

**rmon clear counters**

### Command Mode

Interface Configuration

### Default

None

### Usage

Clear counters on a interface

### Examples

This example shows how to clear rmon counters

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# rmon clear counters
```

## Related Commands

None

## 4.10 debug rmon

Use this command to open rmon debug.

### Command Syntax

**debug rmon**

**no debug rmon**

### Command Mode

Privileged EXEC

### Default

None

### Usage

Open rmon debug

### Examples

This example shows how to open rmon debug

```
Switch# debug rmon
```

## Related Commands

None

# 5 SNMP Commands

## 5.1 snmp-server access

To set the access security of MIB view, use the `snmp-server access` command in global configuration mode. To remove the access security of MIB view, use the `no` form of this command.

### Command Syntax

```
snmp-server access group-name security-model usm (auth | noauth | priv) {context context
(prefix | exact) } | read read-view | write write-view | notify notify-view | }
```

```
no snmp-server access group-name security-model usm (auth | noauth | priv) {context context | }
```

<b>group-name</b>	Name of the group
<b>security-model</b>	Define the security model of the group
<b>usm</b>	SNMPv3 usm security model
<b>auth</b>	Specifies authentication of a packet without encrypting it
<b>noauth</b>	Specifies no authentication of a packe
<b>priv</b>	Specifies authentication of a packet with encryptio
<b>context</b> <i>context</i>	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
<b>prefix</b>	The context only match the prefix
<b>exact</b>	The context should match the whole part
<b>read</b> <i>read-view</i>	Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent
<b>write</b> <i>write-view</i>	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
<b>notify</b> <i>notify-view</i>	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap

## Command Mode

Global Configuration

## Default

No SNMP access group is defined

## Usage

The command is used to create a access security for MIB view.

## Examples

The following is sample output from the snmp-server access command:

```
Switch(config)# snmp-server access manage security-model usm auth write _all_ read _all_
```

## Related Commands

**show snmp-server access**

## 5.2 snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the snmp-server community command in global configuration mode. To remove the specified community string, use the no form of this command.

## Command Syntax

**snmp-server community** *string* (**read-only** | **read-write**) (**view** *view-name* | )

**no snmp-server community** *string*

<i>string</i>	Community string that consists of 1 to 255 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string
<b>read-only</b>	Specifies read-only access. Authorized management stations can retrieve only MIB objects
<b>read-write</b>	Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects
<b>view</b> <i>view-name</i>	Specifies a previously defined view. The view defines the objects available to the SNMP community

## Command Mode

Global Configuration

## Default

No SNMP community string is defined

## Usage

The `no snmp-server` command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

## Examples

The following example shows how to set the read/write community string to `newstring`.

```
Switch(config)# snmp-server community newstring read-write
```

## Related Commands

`snmp-server enable`

## 5.3 snmp-server context

To create a Simple Network Management Protocol (SNMP) context, use the `snmp-server context` command in global configuration mode. To delete an SNMP context, use the `no` form of this command.

## Command Syntax

`snmp-server context context-name`

`no snmp-server context context-name`

<i>context-name</i>	Name of the SNMP context being created
---------------------	----------------------------------------

## Command Mode

Global Configuration

## Default

No SNMP contexts are configured

## Usage

When you use the `no snmp-server context` command, all SNMP instances in that context are deleted.

## Examples

The following is sample output from the `snmp-server context` command:

```
Switch(config)# snmp-server context contextA
```

## Related Commands

**show snmp-server context**

# 5.4 snmp-server enable

To enable the SNMP function, use the `snmp-server enable` command in global configuration mode.

To disable the SNMP function, use the `no` form of this command.

## Command Syntax

**snmp-server enable**

**no snmp-server enable**

## Command Mode

Global Configuration

## Default

SNMP function is disabled

## Usage

The command is used to enable or disable `snmp` global.

## Examples

The following is sample output from the `snmp-server enable` command:

```
Switch(config)# snmp-server enable
```

## Related Commands

**show snmp**

## 5.5 snmp-server engineID

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the `snmp-server engineID` command in global configuration mode. To remove the configured engine ID, use the `no` form of this command.

### Command Syntax

**snmp-server engineID** *engineid-string*

**no snmp-server engineID**

<i>engineid-string</i>	String of a maximum of 64 characters that identifies the engine ID
------------------------	--------------------------------------------------------------------

### Command Mode

Global Configuration

### Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the `show snmp-server engineID` command.

### Usage

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do not need to specify an engine ID for the device. For further details on the SNMP engine ID, see RFC 2571.

### Examples

The following is sample output from the `snmp-server engineID` command:

```
Switch(config)# snmp-server engineID 1234567890
```

### Related Commands

**show snmp-server engineID**

## 5.6 snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the `snmp-server group` command in global configuration mode. To remove a specified SNMP group, use the `no` form of this command.

### Command Syntax

**snmp-server group** *group-name* **user** *user-name* **security-model** **usm**

**no snmp-server group** *group-name* **user** *user-name* **security-model** **usm**

<i>group-name</i>	Name of the group
<b>user</b> <i>user-name</i>	Name of the user in that group
<b>security-model</b>	Define the group security model
<b>usm</b>	SNMPv3 usm model

### Command Mode

Global Configuration

### Default

No SNMP server groups are configured.

### Usage

This command is used to add a new SNMP server group.

### Examples

The following is sample output from the `snmp-server group` command:

```
Switch(config)# snmp-server group SampleA user User1 security-model usm
```

### Related Commands

**show snmp-server group**



## 5.7 snmp-server notify

To set the notification of traps for Simple Network Management Protocol (SNMP), use the `snmp-server notify` command in global configuration mode. To restore to the default value, use the `no` form of this command.

### Command Syntax

**snmp-server notify** *notify-name* **tag** *tag-name* (**inform** | **trap** | )

**no snmp-server notify** *notify-name*

<i>notify-name</i>	Name of the notification
<b>tag</b> <i>tag-name</i>	Name of the tag
<b>inform</b>	Set notify type(default is trap) to INFOR
<b>trap</b>	Set notify type(default is trap) to TRAP

### Command Mode

Global Configuration

### Default

No SNMP notify names are configured

### Usage

This command is used to send events with the notification type of error to the SNMP server.

### Examples

The following is sample output from the `snmp-server notify` command:

```
Switch(config)# snmp-server notify note tag tt
```

### Related Commands

**show snmp-server notify**

## 5.8 snmp-server system-contact

To set the system contact (sysContact) string, use the `snmp-server system-contact` command in global configuration mode. To remove the system contact information, use the `no` form of this command.

### Command Syntax

**snmp-server system-contact** *text*

**no snmp-server system-contact**

<i>text</i>	String that describes the system contact information
-------------	------------------------------------------------------

### Command Mode

Global Configuration

### Default

No system contact string is set

### Usage

This command is used to set the system contact of the SNMP agent so that these descriptions can be accessed through the configuration file.

### Examples

The following is an example of a system contact string:

```
Switch(config)# snmp-server system-contact admin@example.com
```

### Related Commands

**snmp-server system-location**

## 5.9 snmp-server system-location

To set the system location string, use the `snmp-server system-location` command in global configuration mode. To remove the location string, use the `no` form of this command.

## Command Syntax

**snmp-server system-location** *text*

**no snmp-server system-location**

<i>text</i>	String that describes the system contact information
-------------	------------------------------------------------------

## Command Mode

Global Configuration

## Default

No system location string is set

## Usage

This command is used to set the system location of the SNMP agent so that these descriptions can be accessed through the configuration file.

## Examples

The following is an example of a system location string:

```
Switch(config)# snmp-server system-location Sample Place
```

## Related Commands

**snmp-server system-contact**

## 5.10 snmp-server target-address

To specify the recipient of a Simple Network Management Protocol (SNMP) notification message, use the `snmp-server trap target-address` command in global configuration mode. To remove the specified host from the configuration, use the `no` form of this command.

## Command Syntax

**snmp-server target-address** *WORD* **param** *WORD* {**mgmt-if**} (*ipv4-address* | *ipv6-address*)  
(**{udpport** *port* | **timeout** *number* | **retries** *number* } | ) (**taglist** *LINE* | )

**no snmp-server target-address** *WORD* (**mgmt-if**)

<i>WORD</i>	The name of the target address
<b>param</b>	Define a param name which help to find target params table
<i>WORD</i>	The name of the param
<b>mgmt-if</b>	Management port
<i>ipv4-address</i>	IPv4 address
<i>ipv6-address</i>	IPv6 address
<b>community string</b>	Password-like community string sent with the notification operation
<b>udpport port</b>	(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162
<b>timeout numbe</b>	(Optional) The timeout value which area is 0 to 65535, the default is 1500
<b>retries numbe</b>	(Optional) The retry time value which area is 0 to 255, the default is 3
<b>taglist LINE</b>	(Optional) The name of the taglist (128 tags are supported).split by blank.max length is 255 character

## Command Mode

Global Configuration

## Default

No snmp server is configed

## Usage

This command is used to configure a remote manager's IP address.

This command is used for SNMP v3.

## Examples

The following is sample output from the snmp-server target-address command:

```
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist tmptag
```

## Related Commands

**show snmp-server target-address**

## 5.11 snmp-server trap enable

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the `snmp-server trap enable` command in global configuration mode. To disable all available SNMP notifications, use the `no` form of this command.

### Command Syntax

**snmp-server trap enable** *notification-type*

**no snmp-server trap enable** *notification-type*

<i>notification-type</i>	Type of notification to enable or disable. If the all argument is specified, all notifications available on your device are enabled or disabled (if the no form is used)
--------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Command Mode

Global Configuration

### Default

No notifications controlled by this command are sent

### Usage

The `snmp-server trap enable` command is used in conjunction with the `snmp-server trap target-address` command. Use the `snmp-server trap target-address` command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one `snmp-server trap target-address` command.

### Examples

The following is sample output from the `snmp-server trap enable` command:

```
Switch(config)# snmp-server trap enable all
```

### Related Commands

**snmp-server trap target-address**

## 5.12 snmp-server trap delay

To delay snmp-server trap send, use the snmp-server trap delay command in global configuration mode. To disable trap delay, use the no form of this command.

### Command Syntax

**snmp-server trap delay (linkup| linkdown) <1-100>**

**no snmp-server trap delay (linkup| linkdown)**

### Command Mode

Global Configuration

### Default

No delay is enabled

### Usage

The link down and up trap will send immediately while link state change. The command can configure a delay time for link status trap. The unit is 100ms.

### Examples

The following is sample output from the snmp-server trap enable command:

```
Switch(config)# snmp-server trap delay linkup 10
```

### Related Commands

**snmp-server trap target-address**

## 5.13 snmp-server trap target-address

To configure a remote trap manager's IP address, use the snmp-server target-address command in global configuration mode. To remove the configuration, use the no form of this command.

## Command Syntax

**snmp-server trap target-address (mgmt-if | ) (ipv4-address | ipv6-address) community string (udpport number | )**

**no snmp-server trap target-address (mgmt-if | ) (ipv4-address | ipv6-address) community string (udpport number | )**

<b>mgmt-if</b>	Management port
<i>ipv4-address</i>	IPv4 address
<i>ipv6-address</i>	IPv6 address
<b>community string</b>	Password-like community string sent with the notification operation
<b>udpport number</b>	(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162

## Command Mode

Global Configuration

## Default

The router does not send any trap messages.

## Usage

This command is used to specify the server target address to which the trap is sended.

## Examples

The following is sample output from the snmp-server trap target-address command:

```
Switch(config)# snmp-server trap target-address mgmt-if 192.168.1.100 community test udpport 6000
```

## Related Commands

**snmp-server trap enable**

## 5.14 snmp-server inform target-address

To specify the recipient of a Simple Network Management Protocol (SNMP) inform message, use the `snmp-server inform target-address` command in global configuration mode. To remove the specified host from the configuration, use the `no` form of this command.

### Command Syntax

**snmp-server inform target-address** (**mgmt-if** | ) (*ipv4-address* | *ipv6-address*) **community** *string* (**udpport** *number* | )

**no snmp-server inform target-address** (**mgmt-if** | ) (*ipv4-address* | *ipv6-address*) **community** *string* (**udpport** *number* | )

<b>mgmt-if</b>	Management port
<i>ipv4-address</i>	IPv4 address
<i>ipv6-address</i>	IPv6 address
<b>community</b> <i>string</i>	Password-like community string sent with the notification operation
<b>udpport</b> <i>number</i>	(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162

### Command Mode

Global Configuration

### Default

The router does not send any inform messages

### Usage

This command is used to specify the server target address to which the inform is sended.

### Examples

The following is sample output from the `snmp-server inform target-address` command:

```
Switch(config)# snmp-server inform target-address mgmt-if 192.168.1.100 community test udpport 6000
```

### Related Commands

None



## 5.15 snmp-server usm-user

To specify the recipient of a Simple Network Management Protocol (SNMP) notification message, use the `snmp-server trap target-address` command in global configuration mode. To remove the specified host from the configuration, use the `no` form of this command.

### Command Syntax

```
snmp-server usm-user username (remote engine-id |) (authentication (md5 | sha) (8 |)
auth-password (privacy aes | des (8 |) privpassword |) |)
```

```
no snmp-server usm-user username
```

<i>username</i>	Name of the user on the host that connects to the agent
<b>remote</b> <i>engine-id</i>	(Optional) Specifies a remote SNMP entity to which the user belongs
<b>authentication</b>	(Optional) Specifies which authentication level should be used
<b>md5</b>	(Optional) Specifies the HMAC-MD5 authentication level
<b>sha</b>	(Optional) Specifies the HMAC-SHA authentication level
<i>auth-password</i>	(Optional) String that enables the agent to receive packets from the host
<b>privacy</b>	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security
<b>aes</b>	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption
<b>des</b>	(Optional) Specifies the use of the Digital Encryption Standard (DES) algorithm for encryption
<b>8</b>	Specifies a HIDDEN password will follow
<i>privpassword</i>	(Optional) String that specifies the privacy user password

### Command Mode

Global Configuration

### Default

No SNMPv3 users are configured

## Usage

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

## Examples

The following is sample output from the `snmp-server usm-user` command:

```
Switch(config)# snmp-server usm-user user1 authentication md5 mypassword privacy des
yourpassword
```

## Related Commands

`snmp-server engineID`

## 5.16 snmp-server target-params

To specify the SNMP target information to be used in the generation of SNMP messages, use the `snmp-server target-params` in global configuration mode.

### Command Syntax

**snmp-server target-params** *PARAMS* **user** *USER* **security-model v3 message-processing v3**  
(**noauth** | **auth** | **priv**)

**no snmp-server target-params** *PARAMS*

<i>PARAMS</i>	Name of the snmp-server target-params
<b>user</b> <i>USER</i>	Specifies the securityName which identifies the Principal on whose behalf SNMP messages will be generated using this entry
<b>noauth</b>	Need not to authenticate the SNMP message
<b>auth</b>	Need to authenticate the SNMP message, need not to privacy
<b>priv</b>	Need to authenticate and privacy the SNMP message

### Command Mode

Global Configuration

### Default

No target-params are configured

## Usage

The `snmp-server target-params` contains the SNMP target information to be used in the generation of SNMP messages

## Examples

The following is sample output for the `snmp-server target-params` command:

```
Switch(config)# snmp-server target-params param1 user usr1 security-model v3 message-processing v3 noauth
```

## Related Commands

None

## 5.17 snmp-server version

To specify the support of SNMP version, use the `snmp-server version` command in global configuration mode. To restore to the default value, use the `no` form of this command.

### Command Syntax

**snmp-server version (all | v1 | v2c | v3)**

**no snmp-server version**

<b>all</b>	Support all versions (v1, v2c, and v3)
<b>v1</b>	Support only v1 version
<b>v2c</b>	Support only v2c version
<b>v3</b>	Support only v3 version

### Command Mode

Global Configuration

### Default

Support all SNMP versions

## Usage

This command is used to set the SNMP version the switch supported.

## Examples

The following is sample output from the `snmp-server version` command:

```
Switch(config)# snmp-server version all
```

## Related Commands

**show snmp-server version**

## 5.18 snmp-server view

To create or update a view entry, use the `snmp-server view` command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the `no` form of this command.

### Command Syntax

**snmp-server view** *view-name* (**included** | **excluded**) *sub-tree* (**mask** *WORD* | )

**no snmp-server view** *view-name* (**included** | **excluded**) *sub-tree*

<i>view-name</i>	Label for the view record that you are updating or creating. The name is used to reference the record
<b>included</b>	Configures the OID (and subtree OIDs) specified in <i>sub-tree</i> argument to be included in the SNMP view
<b>excluded</b>	Configures the OID (and subtree OIDs) specified in <i>sub-tree</i> argument to be explicitly excluded from the SNMP view
<i>sub-tree</i>	Object identifier of the ASN.1 subtree to be included or excluded from the view
<b>mask</b>	Define the subtree mask

### Command Mode

Global Configuration

## Default

No view entry exists

## Usage

Other SNMP commands require an SMP view as an argument. You use this command to create a view to be used as arguments for other commands.

## Examples

The following is sample output from the snmp-server view command:

```
Switch(config)# snmp-server view abc excluded 1.3.6.2
```

## Related Commands

**show snmp-server view**

## 5.19 snmp-server access-group NAME in

To set the access group, use the snmp-server access-group command in global configuration mode.

To remove the access group, use the no form of this command.

## Command Syntax

**snmp-server access-group *name* in**

**no snmp-server access-group**

<i>name</i>	Access-list name
<b>in</b>	Inbound packets

## Command Mode

Global Configuration

## Default

No access group is defined

## Usage

The command is used to apply ACL in snmp.

## Examples

The following is sample output from the snmp-server access command:

```
Switch(config)# snmp-server access-group abc in
```

## Related Commands

None

## 5.20 show snmp

To display the services information of SNMP, use the show snmp command in privileged EXEC mode.

## Command Syntax

```
show snmp
```

## Command Mode

Privileged EXEC

## Default

None

## Usage

This command is used to display the service information of SNMP (enable or disable).

## Examples

The following is sample output from the show snmp command:

```
Switch# show snmp
```

```
SNMP services: enable
```

## Related Commands

```
snmp-server enable
```

## 5.21 show snmp-server access

To display the ACL information of SNMP, use the show snmp-server access command in privileged EXEC mode.

### Command Syntax

**show snmp-server access** (*group-name*)

<i>group-name</i>	Specify a group name
-------------------	----------------------

### Command Mode

Privileged EXEC

### Default

None

### Usage

This command is used to display the access information configured by command snmp-server access.

### Examples

The following is sample output from the show snmp-server access command:

```
Switch# show snmp-server access gp1
```

```
Group-name      model
=====
Group name:     group1
Context:
Security model: usm
Security level: priv
Context Match:  exact
Read view:      _all_
Write view:     none
Notify view:    none
Storage Type:   permanent
Row status:     active
```

### Related Commands

**snmp-server access**

## 5.22 show snmp-server community

To display the SNMP community information, use the `show snmp-server community` command in privileged EXEC mode.

### Command Syntax

**show snmp-server community**

### Command Mode

Privileged EXEC

### Default

None

### Usage

This command is used to display the community information configured by command `snmp-server community`.

### Examples

The following is sample output from the `show snmp-server community` command:

```
Switch# show snmp-server community
```

```
Community-Access  Community-String  Security-name
=====
read-only         public          comm1
read-write       private        comm2
```

### Related Commands

**snmp-server community**

## 5.23 show snmp-server context

To display the SNMP context information, use the `show snmp-server context` command in privileged EXEC mode.

### Command Syntax

**show snmp-server context**



## Command Mode

Privileged EXEC

## Default

None

## Usage

This command is used to display the context information configured by command `snmp-server context`.

## Examples

The following is sample output from the `show snmp-server context` command:

```
Switch# show snmp-server context
```

```
samplecontext
```

## Related Commands

`snmp-server context`

## 5.24 show snmp-server engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the `show snmp-server engineID` command in EXEC mode.

## Command Syntax

`show snmp-server engineID`

## Command Mode

Privileged EXEC

## Default

None

## Usage

An SNMP engine is a copy of SNMP that can reside on a local or remote device.

## Examples

The following example specifies 0000000902000000c025808 as the local engineID:

```
Switch# show snmp-server engineID
```

```
Engine ID : 0000000902000000c025808
```

## Related Commands

**snmp-server engineID**

## 5.25 show snmp-server group

To display the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group, use the show snmp-server group command in privileged EXEC mode.

## Command Syntax

**show snmp-server group** (*group-name* |)

<i>group-name</i>	Name of the group
-------------------	-------------------

## Command Mode

Privileged EXEC

## Default

None

## Usage

SNMP groups are configured using the snmp-server group command.

## Examples

The following is sample output from the show snmp-server group command:

```
Switch# show snmp-server group
```

```
Group-name      model      Security-name
=====
a11             usm       a
a11             usm       ab
```

## Related Commands

**snmp-server group**

## 5.26 show snmp-server notify

To display notification information of SNMP, use the `show snmp-server notify` command in privileged EXEC mode.

### Command Syntax

**show snmp-server notify** (*notify-name*)

<i>notify-name</i>	Name of the notification
--------------------	--------------------------

### Command Mode

Privileged EXEC

### Default

None

### Usage

This command is used to display the notification information configured by command `snmp-server notify`.

### Examples

The following is sample output from the `show snmp-server notify` command:

```
Switch# show snmp-server notify
```

```
Notify-name      Notify-type
=====
sample          trap
```

### Related Commands

**snmp-server notify**

## 5.27 show snmp-server sys-info

To display the system information of SNMP, use the `show snmp-server sys-info` command in privileged EXEC mode.

### Command Syntax

**show snmp-server sys-info**

### Command Mode

Privileged EXEC

### Default

None

### Usage

The system contact can be set by using the `snmp-server system-contact` command. The system location can be set by using the `snmp-server system-location` command.

### Examples

The following is sample output from the `show snmp-server sys-info` command:

```
Switch# show snmp-server sys-info
```

```
Contact: admin@sampledomain.com
```

```
Location: Denvor
```

### Related Commands

**snmp-server system-contact**

**snmp-server system-location**

## 5.28 show snmp-server trap-receiver

To display the SNMP traps receiver, use the `show snmp-server trap-receiver` command in privileged EXEC mode.

### Command Syntax

**show snmp-server trap-receiver**

## Command Mode

Privileged EXEC

## Default

None

## Usage

This command is used to display traps receiver information configured by command `snmp-server trap target-address`.

## Examples

The following is sample output from the `show snmp-server trap-receiver` command:

Switch# `show snmp-server trap-receiver`

```
Target-ipaddress  udpport  version  pdu-type  community
=====
1.1.1.1           234      v2c     inform   public
1.1.1.1           234      v2c     trap     public
1.1.1.1           234      v1      trap     public
```

## Related Commands

`snmp-server trap target-address`

## 5.29 show snmp-server usm-user

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the `show snmp-server usm-user` command in privileged EXEC mode.

## Command Syntax

`show snmp-server usm-user (username)`

username	(Optional) Name of a specific user or users about which to display SNMP information
----------	-------------------------------------------------------------------------------------

## Command Mode

Privileged EXEC

## Default

None

## Usage

An SNMP user must be part of an SNMP group, as configured using the `snmp-server usm-user` command.

## Examples

The following is sample output from the `show snmp-server usm-user` command:

```
Switch# show snmp-server usm-user user1
```

```
EnginedID: 01234567890123456789
User Name: user1
Auth Protocol: md5
priv Protocol: des
Storage Type: nonvolatile
Row status: active
```

## Related Commands

**snmp-server usm-user**

## 5.30 show snmp-server version

To display the supported version of SNMP, use the `show snmp-server version` command in privileged EXEC mode.

## Command Syntax

**show snmp-server version**

## Command Mode

Privileged EXEC

## Default

None

## Usage

This command is used to display snmp version information configured by command `snmp-server version`.

## Examples

The following is sample output from the show snmp-server version command:

```
Switch# show snmp-server version
```

```
SNMPv1/SNMPv2c/SNMPv3
```

## Related Commands

**snmp-server version**

## 5.31 show snmp-server view

To display the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and associated MIB, use the show snmp-server view command in privileged EXEC mode.

### Command Syntax

**show snmp-server view** (*view-name* |)

<i>view-name</i>	Label for the view record that you are updating or creating. The name is used to reference the record
------------------	-------------------------------------------------------------------------------------------------------

### Command Mode

Privileged EXEC

### Default

None

### Usage

Use this command to display the SNMP view configuration.

## Examples

The following is sample output from the show snmp-server view command:

```
Switch# show snmp-server view
```

```
View-name      View-type      Subtree
=====
abc            excluded      .1.3.6.2
```

all_	included	.0
all_	included	.1
all_	included	.2
none_	excluded	.0
none_	excluded	.1
none_	excluded	.2

## Related Commands

**snmp-server view**



## 6 SFLOW Commands

---

### 6.1 sflow enable

Use this command to enable or disable sFlow globally.

#### Command Syntax

**sflow enable**

**no sflow enable**

#### Command Mode

Global Configuration

#### Defaults

Disabled

#### Usage

Before any other sFlow command can be configured, sFlow services must be enabled globally. Use the no parameter with this command to remove all sFlow configurations and disable sFlow globally.

#### Examples

This example shows how to enable sFlow services globally:

```
Switch# configure terminal
```

```
Switch(config)# sflow enable
```

#### Related Commands

**show sflow**

### 6.2 sflow collector

Use this command to configure sFlow collector.

## Command Syntax

**sflow collector** (*ipv4-address* | *ipv6-address*) (<*1-65535*>|)

**no sflow collector** (*ipv4-address* | *ipv6-address*) (<*1-65535*>|)

<i>ipv4-address</i>	Collector IPv4 address
<i>ipv6-address</i>	Collector IPv6 address
< <i>1-65535</i> >	Collector UDP port number, default is 6343

## Command Mode

Global Configuration

## Defaults

None

## Usage

Use this command to add a collector by specifying the combination of IP address and UDP port. Only up to two unique combinations can be allowed to add. Use the no parameter with this command to delete collector.

## Examples

This example shows how to add a collector with IP address 10.0.0.254 and UDP port 3000.

```
Switch# configure terminal
```

```
Switch(config)# sflow collector 10.0.0.254 3000
```

## Related Commands

**show sflow**

## 6.3 sflow counter interval

Use this command to configure sFlow polling-interval for counter sample.

## Command Syntax

**sflow counter interval** *interval\_id*

**no sflow counter interval**

<i>interval_id</i>	Interval value in second, the range is 1~2000
--------------------	-----------------------------------------------

## Command Mode

Global Configuration

## Defaults

20 seconds

## Usage

Use this command to set sFlow polling-interval for counter sample. Use the no parameter with this command to restore to the default value. Default interval value is 20 seconds.

## Examples

This example shows how to set sFlow polling-interval to 10 second:

```
Switch# configure terminal
```

```
Switch(config)# sflow counter interval 10
```

## Related Commands

**show sflow**

## 6.4 sflow counter enable

Use this command to enable or disable counter sampling on specified port.

## Command Syntax

**sflow counter enable**

**no sflow counter enable**

## Command Mode

Interface Configuration

## Defaults

Disabled

## Usage

Use this command to enable counter sampling on specified port. Use the no parameter with this command to disable counter sampling. By default, sFlow counter sampling is disabled in all ports.

This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

## Examples

This example shows how to enable sFlow counter sampling on interface eth-0-1 and eth-0-2

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# sflow counter enable
```

## Related Commands

**show sflow**

## 6.5 sflow sample rate

Use this command to configure flow sampling rate.

### Command Syntax

**sflow sample rate** *rate\_id*

**no sflow sample rate**

<i>rate_id</i>	Sample rate value, must be a power of 2, the range is 1~32768
----------------	---------------------------------------------------------------

### Command Mode

Interface Configuration

### Defaults

8192

### Usage

Use this command to set sFlow packet sampling rate. Use no parameter with this command to set default sampling rate. Default sampling rate value is 8192.

sFlow uses CPU resources to collect samples and send samples to the collector. If a low sampling rate is set, CPU utilization can become high. To protect CPU from overwhelming, exceeded flow samples would be dropped. If a sampling rate less than default value is configured, a prompt will be given to info the potential of involving a high CPU utilization.

This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

## Examples

This example shows how to set the sFlow sampling rate to 2048 on eth-0-1:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# sflow sample rate 2048
```

```
% Warning: sFlow sampling requires high CPU usage, especially with a low rate.  
It is suggested not configure a rate less than default value 8192.
```

## Related Commands

**show sflow**

## 6.6 sflow sample enable

Use this command to enable or disable packet sampling on individual port.

### Command Syntax

**sflow sample enable input**

**no sflow sample enable input**

### Command Mode

Interface Configuration

### Defaults

Disabled

### Usage

Use this command to enable ingress direction of packet sampling on individual port. Use the no parameter with this command to disable packet sampling. By default, sFlow packet sampling is disabled in all ports.

This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

## Examples

This example shows how to enable input packet sampling on route port eth-0-1:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# sflow sample enable input
```

## Related Commands

**show sflow**

## 6.7 show sflow

Use this command to show the running information of sflow.

### Command Syntax

**show sflow**

### Command Mode

Privileged EXEC

### Defaults

None

### Usage

Use this command to show the running information of sflow.

## Examples

This example shows how to show the sflow running information:

```
Switch# show sflow
```

```
sFlow Global Information:
```

```
Agent IP address      : 0.0.0.0
```

```
Counter Sampling Interval : 20 seconds
```

```
Collector IP         : Not configured
```

```
sFlow Port Information:
```

		Sample	Sample	
Port	Counter	Sample	Direction	Rate
-----				
eth-0-1	Disable	Enable	Input	8192

## Related Commands

**sflow enable**

**sflow collector**

**sflow counter interval**

**sflow counter enable**

**sflow sample rate**

**sflow sample enable**

# 7 LLDP Commands

---

## 7.1 lldp enable(global)

To enable LLDP function globally, use the `lldp enable` command in global configuration mode. To disable this function, use the `no` form of this command.

### Command Syntax

`lldp enable`

`lldp disable`

### Command Mode

Global Configuration

### Default

LLDP is disabled globally.

### Usage

The LLDP function will start to work after being enabled globally and on special interface.

### Examples

The following example shows how to enable LLDP globally:

```
Switch(config)# lldp enable
```

### Related Commands

`lldp enable(interface)`

## 7.2 lldp enable(interface)

To enable LLDP function on interface, use the `lldp enable` command in interface configuration mode. To disable this function, use the `no` form of this command.



## Command Syntax

**lldp enable (txonly|txrx|rxonly)**

**lldp disable**

<b>txonly</b>	Enable lldp pdu transmission
<b>txrx</b>	Enable lldp pdu transmission and reception
<b>rxonly</b>	Enable lldp pdu reception

## Command Mode

Interface Configuration

## Default

LLDP is disabled on the interface.

## Usage

This command is used to specify the remote DHCPv6 server or relay.

## Examples

The following example shows how to enable LLDP on interface:

```
Switch(config-if)# lldp enable txrx
```

## Related Commands

**lldp enable(global)**

## 7.3 lldp system-name

To configure system name for System Name TLV, use the `lldp system-name` command in global configuration mode. To restore the default configuration, use the `no` form of this command.

## Command Syntax

**lldp system-name** *NAME*

**no lldp system-name**

<i>NAME</i>	System Name. The range is from 1 to 64
-------------	----------------------------------------

## Command Mode

Global Configuration

## Default

Default system name is used.

## Usage

If no system name is configured, the default system name will be used.

## Examples

The following example shows how to configure system name:

```
Switch(config)# lldp system-name switch
```

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.4 lldp system-description

To configure system description for System Description TLV, use the `lldp system-description` command in global configuration mode. To restore the default configuration, use the `no` form of this command.

## Command Syntax

**lldp system-description** *LINE*

**no lldp system-description**

<i>LINE</i>	System Description. The range is from 1 to 255 and space is allowed
-------------	---------------------------------------------------------------------

## Command Mode

Global Configuration

## Default

Default system description is used.

## Usage

If no system description is configured, the default system description will be used.

## Examples

The following example shows how to configure system description:

```
Switch(config)# lldp system-description switch
```

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.5 lldp management ip

To configure management ip address for Management Address TLV, use the lldp management ip command in global configuration mode. To restore the default configuration, use the no form of this command.

### Command Syntax

**lldp management ip** *ADDRESS*

**no lldp management ip**

<i>ADDRESS</i>	IPv4 address, like 1.1.1.1
----------------	----------------------------

### Command Mode

Global Configuration

### Default

Default management address is used.

## Usage

If Management Address not be configured, system should use the management IP address, IP address of the transmitting interface or MAC address of the transmitting interface according descend order of priority.

## Examples

The following example shows how to configure the management ip address.

```
Switch(config)# lldp management ip 192.168.1.2
```

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.6 lldp msg-tx-hold

To configure msg-tx-hold, use the lldp msg-tx-hold command in global configuration. To restore the default configuration, use the no form of this command.

### Command Syntax

**lldp msg-tx-hold** *NUMBER*

**no lldp msg-tx-hold**

<i>NUMBER</i>	The range is from 2 to 10
---------------	---------------------------

### Command Mode

Global Configuration

### Default

The default value of msg-tx-hold is 4.

### Usage

None

## Examples

The following example shows how to configure msg-tx-hold:

```
Switch(config)# lldp msg-tx-hold 3
```

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.7 lldp timer msg-tx-interval

To configure msg-tx-interval, use the lldp timer msg-tx-interval command in global configuration. To restore the default configuration, use the no form of this command.

### Command Syntax

**lldp timer msg-tx-interval** *NUMBER*

**no lldp timer msg-tx-interval**

<i>NUMBER</i>	The range is from 5 to 32768
---------------	------------------------------

### Command Mode

Global Configuration

### Default

The default value of msg-tx-interval is 30s.

### Usage

None

## Examples

The following example shows how to configure msg-tx-interval:

```
Switch(config)# lldp timer msg-tx-interval 20
```

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.8 lldp timer reinit-delay

To configure reinitDelay, use the lldp timer reinitDelay command in global configuration. To restore the default configuration, use the no form of this command.

### Command Syntax

**lldp timer reinit-delay***NUMBER*

**no lldp timer reinit-delay**

<i>NUMBER</i>	The range is from 1 to 10
---------------	---------------------------

### Command Mode

Global Configuration

### Default

The default value of reinitDelay is 2s.

### Usage

None

### Examples

The following example shows how to configure reinitDelay:

```
Switch(config)# lldp timer reinit-delay 1
```

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.9 lldp timer tx-delay

To configure tx-delay, use the lldp timer tx-delay command in global configuration. To restore the default configuration, use the no form of this command.

### Command Syntax

**lldp timer tx-delay** *NUMBER*

**no lldp timer tx-delay**

<i>NUMBER</i>	The range is from 1 to 8192
---------------	-----------------------------

### Command Mode

Global Configuration

### Default

The default value of tx-delay is 2s.

### Usage

The value of tx-delay should obey the formula:  $1 \leq \text{tx-delay} \leq ((0.25) * \text{msg-tx-interval})$ .

### Examples

The following example shows how to configure tx-delay:

```
Switch(config)# lldp timer tx-delay 3
```

### Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.10 lldp tlv basic

To select the basic tlv used in LLDP packet, use the lldp tlv basic command in interface configuration. To cancel the tlv, use the no form of this command..

## Command Syntax

**lldp tlv basic** ({ port-description | system-name | system-description | system-capabilities | management-address} | all)

**no lldp tlv basic** ({ port-description | system-name | system-description | system-capabilities | management-address} | all)

<b>port-description</b>	Select Port Description Tlv
<b>system-name</b>	Select System Name Tlv
<b>system-description</b>	Select System Description Tlv
<b>system-capabilities</b>	Select System Capabilities Tlv
<b>management-address</b>	Select Management Address Tlv
<b>all</b>	Select All basic tlvs

## Command Mode

Interface Configuration

## Default

All basic tlvs is selected.

## Usage

None

## Examples

The following example shows how to select basic tlv:

```
Switch(config-if)# lldp tlv basic system-name
```

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**



## 7.11 lldp tlv 8021-org-specific

To select the IEEE 802.1 tlv used in LLDP packet, use the `lldp tlv 8021-org-specific` command in interface configuration. To cancel the tlv, use the no form of this command..

### Command Syntax

`lldp tlv 8021-org-specific` (`{port-vlan | protocol-vlan | vlan-name | protocol-id | link-aggregation }` |all)

`no lldp tlv 8021-org-specific` (`{port-vlan | protocol-vlan | vlan-name | protocol-id | link-aggregation }` |all)

<b>port-vlan</b>	Select Port Vlan ID Tlv
<b>protocol-vlan</b>	Select Port and Protocol Vlan ID Tlv
<b>vlan-name</b>	Select Vlan Name Tlv
<b>protocol-id</b>	Select Protocol Identity Tlv
<b>link-aggregation</b>	Select Link Aggregation Tlv
<b>all</b>	Select All IEEE 802.1 tlv, exclude Link Aggregation Tlv

### Command Mode

Interface Configuration

### Default

All IEEE 802.1 tlv is selected, exclude Link Aggregation Tlv.

### Usage

Link Aggregation Tlv in IEEE 802.3 tlv set is used by default.

### Examples

The following example shows how to select IEEE 802.1 tlv :

```
Switch(config-if)# lldp tlv 8021-org-specific vlan-name
```

### Related Commands

`lldp enable(global)`

`lldp enable(interface)`

## 7.12 lldp tlv 8023-org-specific

To select the IEEE 802.3 tlv used in LLDP packet, use the `lldp tlv 8023-org-specific` command in interface configuration. To cancel the tlv, use the no form of this command.

### Command Syntax

`lldp tlv 8023-org-specific ({mac-phy-cfg | power | link-aggregation | max-frame-size } | all)`

`no lldp tlv 8023-org-specific ({mac-phy-cfg | power | link-aggregation | max-frame-size } | all)`

<b>mac-phy-cfg</b>	Select MAC/PHY Configuration/Status TLV
<b>power</b>	Select Power Via MDI Tlv
<b>link-aggregation</b>	Select Link Aggregation Tlv
<b>max-frame-size</b>	Select Maximum Frame Size Tlv
<b>all</b>	Select All IEEE 802.3 tlv

### Command Mode

Interface Configuration

### Default

All IEEE 802.3 tlv is selected.

### Usage

Link Aggregation Tlv in IEEE 802.3 tlv set is used by default.

### Examples

The following example shows how to select IEEE 802.3 tlv :

```
Switch(config-if)# lldp tlv 8023-org-specific power
```

### Related Commands

`lldp enable(global)`

`lldp enable(interface)`

## 7.13 lldp tlv med

To select the MED tlvs used in LLDP packet, use the `lldp tlv med` command in interface configuration. To cancel the tlv, use the `no` form of this command..

### Command Syntax

**lldp tlv med** ({network-policy | ext-power | inventory} | all)

**no lldp tlv med** ({network-policy | ext-power | inventory }| all)

<b>network-policy</b>	Select Network Policy TLV
<b>ext-power</b>	Select Extend Power-Via-MDI Tlv
<b>inventory</b>	Select Inventory Tlv
<b>all</b>	Select All MED tlvs, exclude Location Identification Tlv

### Command Mode

Interface Configuration

### Default

All MED tlvs is selected, exclude Location Identification Tlv.

### Usage

LLDP-MED Capabilities TLV will be added automatically when any other tlv in MED tlv set was selected, and canceled when no other MED tlv except itself was selected.

### Examples

The following example shows how to select MED tlv :

```
Switch(config-if)# lldp tlv med inventory
```

### Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.14 debug lldp

Use this command to turn on the debug switches of LLDP module.

To restore the default, use the **no** form of this command

### Command Syntax

**debug lldp ( events | packet | all )**

**no debug lldp ( events | packet | all )**

<b>events</b>	LLDP events
<b>packet</b>	LLDP Packet information
<b>all</b>	Turn all debugging on

### Command Mode

Privileged EXEC

### Default

None

### Usage

Use command “terminal monitor ” to make debug messages print on the VTY immediately.

Use command “show logging buffer” to check the debug messages in the logging buffer.

### Examples

The following is sample to open lldp debug switches:

```
Switch# debug lldp all
```

### Related Commands

**terminal monitor**

**show logging buffer**

## 7.15 show lldp local

To display the LLDP local information, use the show lldp local command in privileged EXEC mode.

### Command Syntax

**show lldp local (config | tlv-info) (interface *IFNAME* |)**

<b>config</b>	Configuration Information
<b>tlv-info</b>	Local LLDP TLV information
<b>interface</b>	Display LLDP configuration or tlv information of special interface
<i>IFNAME</i>	Interface name, only allowed physical interface

### Command Mode

Privileged EXEC

### Default

None

### Usage

If interface is not specified, this command will display the global information of LLDP.

### Examples

The following example shows how to display LLDP configuration:

```
Switch# show lldp local config
```

```
LLDP global configuration:
=====
LLDP function global enabled : NO
LLDP msgTxHold      : 4
LLDP msgTxInterval  : 30
LLDP reinitDelay    : 2
LLDP txDelay        : 2
```

```
Switch# show lldp local config interface eth-0-4
```

```
LLDP configuration on interface eth-0-4 :
=====
LLDP admin status : Disabled

Basic optional TLV Enabled:
  Port Description TLV
```

System Name TLV  
System Description TLV  
System Capabilities TLV  
Management Address TLV

IEEE 802.1 TLV Enabled:

Port Vlan ID TLV  
Port and Protocol Vlan ID TLV  
Vlan Name TLV  
Protocol Identity TLV

IEEE 802.3 TLV Enabled:

MAC/PHY Configuration/Status TLV  
Power Via MDI TLV  
Link Aggregation TLV  
Maximum Frame Size TLV

LLDP-MED TLV Enabled:

Med Capabilities TLV  
Network Policy TLV  
Extended Power-via-MDI TLV  
Inventory TLV

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

**lldp tlv basic**

**lldp tlv med**

**lldp tlv 8023-org-specific**

**lldp tlv 8021-org-specific**

**lldp msg-tx-hold**

**lldp timer msg-tx-interval**

**lldp timer reinitDelay**

**lldp timer tx-delay**

## 7.16 show lldp neighbor

To display LLDP neighbor information, use the `show lldp neighbor` command in privileged EXEC mode.

### Command Syntax

**show lldp neighbor (interface *IFNAME* |) (brief |)**

<b>interface</b>	Display LLDP neighbor information of special interface
<i>IFNAME</i>	Interface name, only allowed physical interface
<b>brief</b>	Display brief information

## Command Mode

Privileged EXEC

## Default

None

## Usage

This command is used to display the LLDP neighbor information.

## Examples

The following example shows how to display LLDP neighbor information:

```
Switch# show lldp neighbor interface eth-0-4 brief
```

```
Local Port : eth-0-4  
Remote Port : eth-0-6  
Hold Time : 120  
Expire Time : 116  
System Name : switch
```

---

## Related Commands

**lldp enable(global)**

**lldp enable(interface)**

## 7.17 show lldp statistics

To display the statistics of LLDP packets, use the show lldp statistics command in privileged EXEC mode.

## Command Syntax

**show lldp statistics (interface *IFNAME* )**

<b>interface</b>	Display LLDP statistics of special interface
<i>IFNAME</i>	Interface name, only allowed physical interface

## Command Mode

Privileged EXEC

## Default

None

## Usage

This command is used to display detail LLDP statistics.

## Examples

The following example shows how to display LLDP statistics:

```
Switch# show lldp statistics interface eth-0-4
```

```
LLDP statistics information:
=====
LLDP Port statistics for eth-0-4
Frames transmitted: 568
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Recieved: 364
TLVs discarded: 0
TLVs unrecognized: 0
```

## Related Commands

**clear lldp statistics**

## 7.18 clear lldp statistics

To reset the statistics of LLDP packets , use the clear lldp statistics command in privileged EXEC mode.

## Command Syntax

**clear lldp statistics (interface *IFNAME* )**



<b>interface</b>	Clear LLDP statistics of special interface
<i>IFNAME</i>	Interface name, only allowed physical interface

## Command Mode

Privileged EXEC

## Default

None

## Usage

This command is used to reset LLDP statistics.

## Examples

The following example shows how to clear LLDP statistics:

```
Switch# clear lldp statistics
```

## Related Commands

**show lldp statistics**