FSOS

Network Management Command Line Reference

Contents

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** | **mgmt-if** | **ipv6**| **vrf** *WORD* |) *WORD*

ip	Public network IPv4 echo
vrf *WORD*	VPN Routing/Forwarding instance
mgmt-if	Management interface
WORD	Ping destination IPv4 or IPv6 address or hostname
ipv6	Public network IPv6 echo

interface	Outgoing interface for LinkLocal address/host
IFNAME	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*

ip	Public network IPv4 echo
ipv6	Public network IPv6 echo
vrf *WORD*	VPN Routing/Forwarding instance
mgmt-if	Management interface
WORD	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** *A.B.C.D*|) (**version** | **kod** | **ignore** | **noquery** | **nomodify** | **notrap** | **noserve** | **nopeer** | **notrust** | **limited** | **none**)

no ntp ace (*address* | *hostname*) (**mask** *A.B.C.D*|) (**version** | **kod** | **ignore** | **noquery** | **nomodify** | **notrap** | **noserve** | **nopeer** | **notrust** | **limited** | **none**)

address	IP address of the time server or peer
hostname	Name of the time server or peer
mask *A.B.C.D*	Specify network mask of the address
version	Ignore these hosts if not the current NTP version
kod	If access is denied, send a kiss-of-death packet
ignore	Ignore all packets from host that match this entry
noquery	Ignore all NTP mode 6 and 7 packets from the source, time service is not affected
nomodify	Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server
notrap	Decline to provide mode 6 control message trap service to matching hosts

noserve	Ignore NTP packets whose mode is other than 6 or 7
nopeer	Provide stateless time service to polling hosts, but do not allocate peer memory resources
notrust	Treat these hosts normally in other respects, but never use them as synchronization sources
limited	These hosts are subject to limitation of number of clients from the same net
none	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)

enable	Enable NTP authentication
disable	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 enables 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

delay	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)# interface eth-0-1

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 receive 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*

keyid	Authentication key (1 to 64000)
value	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*)

hostname	Name of the time server or peer
address	IP address of the time server or peer
key *key-id*	Authentication key to use when sending packets to this peer (1 to 64000)
prefer	Makes this peer the preferred peer that provides synchronization
version *number*	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

number	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*)

hostname	Name of the time server or peer
address	IP address of the time server or peer
key *key-id*	Authentication key to use when sending packets to this peer (1 to 64000)
prefer	Makes this peer the preferred peer that provides synchronization
version *number*	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*

key-id	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, - outlyer
```

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 a 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**)

internal *IFPHYSICAL*	Packets transmitted to the interface should be looped back to a specified physical interface without any modification. The destination physical interface
external	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|)

mac-address swap	If this flied 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

loopback phy

loopback port

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

loopback phy

loopback port

3.5 l2 ping

Use this command to ping specified DMAC from specified physical interface, using protocol packet with ethertype 0x9009.

Command Syntax

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

HHHH.HHHH.HHHH	The DMAC to ping
IFPHYSICAL	The interface to ping from
vlan <1-4094>	The vlan id of the protocol ping packet
interval *<1-65535>*	The interval time between two ping action, millisecond
timeout *<1-65535>*	The time wait for a ping action, millisecond
count *<1-65535>*	Total ping times
size <64-1518>	The size of the protocol ping packet

Command Mode

Privileged EXEC

Defaults

The ping protocol packet is without vlan tag by default.

The default interval ping time is 200 milliseconds.

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# l2 ping 0000.0000.0001 interface eth-0-1 vlan 101 interval 200 timeout 1000 count 10 size 1500

Related Commands

l2 ping response

3.6 l2 ping response

Use this command to enable l2 ping response globally. Use the no form of this command to disable it.

Command Syntax

l2 ping response enable

no l2 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)

all	All packet

packet	Packet
send	Send packets
receive	Receive packets
response	Response Log

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 debugging:

Switch# show debugging l2ping

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

Related Commands

l2 ping response

4 RMON 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*

ID	Specify the RMON group of statistics. The range is 1~65535
owner *WORD*	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*

Index	Specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1~65535
buckets *numbs*	Specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1~65535
interval *values*	Specify the number of seconds in each polling cycle. The range is 1~*3600*
owner *WORD*	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 an event to RMON event table

Command Syntax

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

no rmon event *Index*

Index	Event index. The range is 1~65535

log	Generate a RMON log when event is triggered
trap *WORD*	Trap community
description *WORD*	Specify the description string for the event (default is RMON_SNMP)
owner *WORD*	The owner name (default is RMON_SNMP)

Command Mode

Global Configuration

Default

None

Usage

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

Examples

This example shows how to create an 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 an 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*

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

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

Examples

This example shows how to set an 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* |)

statistics_id	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* |)

history_id	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* |)

event_id	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* |)

alarm_id	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 rmon debug

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* | }

group-name	Name of the group
security-model	Define the security model of the group
usm	SNMPv3 usm security model
auth	Specifies authentication of a packet without encrypting it
noauth	Specifies no authentication of a packet
priv	Specifies authentication of a packet with encryption
context *context*	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
prefix	The context only match the prefix
exact	The context should match the whole part

read *read-view*	Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent
write *write-view*	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
notify *notify-view*	(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*

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community strin
read-only	Specifies read-only access. Authorized management stations can retrieve only MIB objects
read-write	Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects
view *view-name*	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*

context-name	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

engineid-string	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**

group-name	Name of the group
user *user-name*	Name of the user in that group
security-model	Define the group security model
usm	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*

notify-name	Name of the notification
tag *tag-name*	Name of the tag
inform	Set notify type(default is trap) to INFOR
trap	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

text	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@exampledomain.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

text	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**|)

WORD	The name of the target address
param	Define a param name which help to find target params table
WORD	The name of the param
mgmt-if	Management port
ipv4-address	IPv4 address
ipv6-address	IPv6 address

community *string*	Password-like community string sent with the notification operation
udpport *port*	(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162
timeout *numbe*	(Optional) The timeout value which area is 0 to 65535, the default is 1500
retries *numbe*	(Optional) The retry time value which area is 0 to 255, the default is 3
taglist *LINE*	(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 configured.

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*

notification-type	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* |)

mgmt-if	Management port
ipv4-address	IPv4 address
ipv6-address	IPv6 address
community *string*	Password-like community string sent with the notification operation
udpport *number*	(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 sent.

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* |)

mgmt-if	Management port
ipv4-address	IPv4 address
ipv6-address	IPv6 address
community *string*	Password-like community string sent with the notification operation
udpport *number*	(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 sent.

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-passsword* (**privacy** (**aes** | **des)** (8 |) *privpassword* |) |)

no snmp-server usm-user *username*

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

all	Support all versions (v1, v2c, and v3)
v1	Support only v1 version
v2c	Support only v2c version
v3	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

5.17 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*

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

5.18 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**

name	Access-list name
in	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

5.19 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

5.20 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*|)

group-name	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

5.21 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

5.22 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

5.23 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 000000090200000000c025808 as the local engineID:

Switch# show snmp-server engineID

```
Engine ID  : 000000090200000000c025808
```

Related Commands

snmp-server engineID

5.24 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*|)

group-name	Specify a group name

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

5.25 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 (*group-name*|)

group-name	Specify a group name

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

5.26 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

5.27 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-addres.

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-addres

5.28 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

5.29 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

5.30 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*|)

view-name	Specify a view name

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 agent

Use this command to configure sFlow agent.

Command Syntax

sflow agent (**ip** *ipv4-address* | **ipv6** *ipv6-addres*)

no sflow agent (ip | ipv6)

ipv4-address	Agent IPv4 address
ipv6-address	Agent IPv6 address

Command Mode

Global Configuration

Defaults

None

Usage

Use this command to configure IP address for sflow agent. If not configured and router-id has configured, sflow will use the first valid router-id and then never change.

Examples

This example shows how to configure agent with IP address 10.0.0.254.

Switch# configure terminal

Switch(config)# sflow agent ip 10.0.0.254

Related Commands

show sflow

6.3 sflow collector

Use this command to configure sFlow collector.

Command Syntax

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

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

ipv4-address	Collector IPv4 address
ipv6-address	Collector IPv6 address
<1-65535>	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

6.4 sflow counter interval

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

Command Syntax

sflow counter interval *interval_val*

no sflow counter interval

interval_val	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

6.5 sflow counter-sampling enable

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

Command Syntax

sflow counter-sampling enable

no sflow counter-sampling 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-sampling enable

Related Commands

show sflow

6.6 sflow flow-sampling rate

Use this command to configure flow sampling rate.

Command Syntax

sflow flow-sampling rate *rate_val*

no sflow flow-sampling rate

rate_val	Sample rate value, must be a power of 2, the range is 1~8192

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 flow-sampling 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

6.7 sflow flow-sampling enable

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

Command Syntax

sflow flow-sampling enable (input|output|both)

no sflow flow-sampling enable (input|output|both)

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 flow-sampling enable input

Related Commands

show sflow

6.8 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:
                                  Flow-Sample   Flow-Sample
 Port       Counter     Flow      Direction     Rate
 ---------------------------------------------------------
 eth-0-1     Disable     Enable   Input          8192
```

Related Commands

sflow enable

sflow collector

sflow counter interval

sflow counter-sampling enable

sflow flow-sampling rate

sflow flow-sampling 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

txonly	Enable lldp pdu transmission
txrx	Enable lldp pdu transmission and reception
rxonly	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

NAME	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

LINE	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

ADDRESS	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

NUMBER	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

NUMBER	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

NUMBER	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

NUMBER	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 <= tx-delay <= ((0.25)* 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}

port-description	Select Port Description Tlv
system-name	Select System Name Tlv
system-description	Select System Description Tlv
system-capabilities	Select System Capabilities Tlv
management-address	Select Management Address Tlv
all	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 tlvs 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}

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

Command Mode

Interface Configuration

Default

All IEEE 802.1 tlvs 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 tlvs 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}

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

Command Mode

Interface Configuration

Default

All IEEE 802.3 tlvs 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}

network-policy	Select Network Policy TLV

ext-power	Select Extend Power-Via-MDI Tlv
inventory	Select Inventory Tlv
all	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)

events	LLDP events
packet	LLDP Packet information
all	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* **|)**

config	Configuration Information
tlv-info	Local LLDP TLV information
interface	Display LLDP configuration or tlv information of special interface
IFNAME	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 |)**

interface	Display LLDP neighbor information of special interface
IFNAME	Interface name， only allowed physical interface
brief	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* **|)**

interface	Display LLDP statistics of special interface
IFNAME	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* **|)**

interface	Clear LLDP statistics of special interface
IFNAME	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