FiberstoreOS

Network Management Configuration Guide

Contents

Figures

1 Configuring Network Diagnosis

1.1 Overview

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) [1] and records any packet loss. The results of the test are printed in form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

Traceroute is a computer network tool for measuring the route path and transit times of packets across an Internet Protocol (IP) network.

Traceroute sends a sequence of Internet Control Message Protocol (ICMP) packets addressed to a destination host. Tracing the intermediate routers traversed involves control of the time-to-live (TTL) Internet Protocol parameter. Routers decrement this parameter and discard a packet when the TTL value has reached zero, returning an ICMP error message (ICMP Time Exceeded) to the sender.

1.2 Configurations

Ping IP with inner port

Switch# ping 10.10.29.247	Ping IP 10.10.29.247 with inner port
Switch# ping ipv6 2001:1000::1	Ping IP 2001:1000::1 with inner port

Ping IP with management port

Switch# ping mgmt-if 10.10.29.247	Ping IP 10.10.29.247 with management port
Switch# ping mgmt-if ipv6 2001:1000::1	Ping IP 2001:1000::1 with management port

Ping IP with VRF instance

Switch# ping vrf vrf1 10.10.10.1	Ping IP 10.10.10.1 with VRF vrf1 instance

Traceroute IP with inner port

Switch# traceroute 1.1.1.2	Traceroute IP 1.1.1.2 with inner port
Switch# traceroute ipv6 2001:1000::1	Traceroute IP 2001:1000::1 with inner port

1.3 Validation

```
Switch# ping mgmt-if 192.168.100.101
PING 192.168.100.101 (192.168.100.101) 56(84) bytes of data.
64 bytes from 192.168.100.101: icmp_seq=0 ttl=64 time=0.092 ms
64 bytes from 192.168.100.101: icmp_seq=1 ttl=64 time=0.081 ms
64 bytes from 192.168.100.101: icmp_seq=2 ttl=64 time=0.693 ms
64 bytes from 192.168.100.101: icmp_seq=3 ttl=64 time=0.071 ms
64 bytes from 192.168.100.101: icmp_seq=4 ttl=64 time=1.10 ms

--- 192.168.100.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.071/0.408/1.104/0.421 ms, pipe 2
```

```
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)  112.465 ms  102.257 ms  131.948 ms
```

```
Switch # ping mgmt-if ipv6 2001:1000::1
PING 2001:1000::1(2001:1000::1) 56 data bytes
64 bytes from 2001:1000::1: icmp_seq=1 ttl=64 time=0.291 ms
```

```
64 bytes from 2001:1000::1: icmp_seq=2 ttl=64 time=0.262 ms
64 bytes from 2001:1000::1: icmp_seq=3 ttl=64 time=0.264 ms
64 bytes from 2001:1000::1: icmp_seq=4 ttl=64 time=0.270 ms
64 bytes from 2001:1000::1: icmp_seq=5 ttl=64 time=0.274 ms

--- 2001:1000::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.262/0.272/0.291/0.014 ms
Switch #
```

2 Configuring NTP

2.1 Overview

NTP is a tiered time distribution system with redundancy capability. NTP measures delays within the network and within the algorithms on the machine on which it is running. Using these tools and techniques, it is able to synchronize clocks to within milliseconds of each other when connected on a Local Area Network and within hundreds of milliseconds of each other when connected to a Wide Area Network. The tiered nature of the NTP time distribution tree enables a user to choose the accuracy needed by selecting a level (stratum) within the tree for machine placement. A time server placed higher in the tree (lower stratum number), provides a higher likelihood of agreement with the UTC time standard.

Some of the hosts act as time servers, that is, they provide what they believe is the correct time to other hosts. Other hosts act as clients, that is, they find out what time it is by querying a time server. Some hosts act as both clients and time servers, because these hosts are links in a chain over which the correct time is forwarded from one host to the next. As part of this chain, a host acts first as a client to get the correct time from another host that is a time server. It then turns around and functions as a time server when other hosts, acting as clients, send requests to it for the correct time.

2.2 Topology

Figure 2-1 NTP server-client with authentication topology

Before configuring NTP client, make sure that NTP service is enabled on Server.

2.3 Configurations

Configuring interface vlan10

Switch# configure terminal	Enter the Configure mode.
Switch(config)# vlan database	Enter the vlan database Configure mode.
Switch(config-vlan)# vlan 10	Add vlan 10 to database
Switch(config-vlan)# exit	Exit the vlan database configuration mode
Switch(config)# interface eth-0-26	Enter the interface configuration mode
Switch(config-if)# switch access vlan 10	Add port to vlan 10
Switch(config-if)# no shutdown	Up the interface eth-0-26
Switch(config-if)# exit	Exit the interface configuration mode
Switch(config)# interface vlan10	Enter the vlan interface configuration mode
Switch(config-if)# ip address 6.6.6.5/24	Set IP address
Switch(config-if)# exit	Exit the vlan interface configuration mode

Configuring NTP client

Switch(config)# ntp key 1 serverkey	Enable a trustedkey
Switch(config)# ntp server 6.6.6.6 key 1	Configure the IP address of the NTP server
Switch(config)# ntp authentication enable	Enable authentication

Switch(config)# ntp trustedkey 1	Once you have enabled authentication, the client switch sends the time-of-day requests to the trusted NTP servers only
Switch(config)# ntp ace 6.6.6.6 none	Configure ntp ace

Configuring NTP Server

Step 1 Display eth1 ip address

```
[root@localhost octeon]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:08:C7:89:4B:AA
          inet addr:6.6.6.6  Bcast:6.6.6.255  Mask:255.255.255.0
          inet6 addr: fe80::208:c7ff:fe89:4baa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3453 errors:1 dropped:0 overruns:0 frame:1
          TX packets:3459 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:368070 (359.4 KiB)  TX bytes:318042 (310.5 KiB)
```

Step 2 Check networks via Ping

```
[root@localhost octeon]# ping 6.6.6.5
PING 6.6.6.5 (6.6.6.5) 56(84) bytes of data.
64 bytes from 6.6.6.5: icmp_seq=0 ttl=64 time=0.951 ms
64 bytes from 6.6.6.5: icmp_seq=1 ttl=64 time=0.811 ms
64 bytes from 6.6.6.5: icmp_seq=2 ttl=64 time=0.790 ms
```

Step 3 Configure ntp.conf

```
[root@localhost octeon]# vi /etc/ntp.conf
server  127.127.1.0 # local clock
fudge   127.127.1.0 stratum 5

#
# Drift file.  Put this in a directory which the daemon can write to.
# No symbolic links allowed, either, since the daemon updates the file
# by creating a temporary in the same directory and then rename()'ing
# it to the file.
#
driftfile /var/lib/ntp/drift
broadcastdelay  0.008
broadcast 6.6.6.255
#
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will. Note also that
# ntpd is started with a -A flag, disabling authentication, that
# will have to be removed as well.
#
#disable auth
keys        /etc/ntp/keys
trustedkey 1
```

Step 4 Configure keys

```
[root@localhost octeon]# vi /etc/ntp/keys
#
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will. Note also that
# ntpd is started with a -A flag, disabling authentication, that
# will have to be removed as well.
#
1 M serverkey
```

Step 5 Start ntpd service

```
[root@localhost octeon]# ntpd
```

2.4 Validation

Switch# show ntp

```
Current NTP configuration:
============================================================
NTP access control list:
  6.6.6.6 none
Unicast peer:
Unicast server:
  6.6.6.6 key 1
Authentication: enabled
Local reference clock:
```

```
Switch# show ntp status
Current NTP status:
============================================================
clock is synchronized
stratum:         7
reference clock: 6.6.6.6
frequency:       17.365 ppm
precision:       2**20
reference time:  d14797dd.70b196a2  ( 1:54:37.440 UTC   Thu Apr  7 2011)
root delay:      0.787 ms
root dispersion: 23.993 ms
peer dispersion: 57.717 ms
clock offset:    -0.231 ms
stability:       6.222 ppm
```

```
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   50  128   37      0.778   -0.234  71.945
```

```
* synchronized, + candidate, # selected, x falsetick, . excess, - outlier
```

NOTE

If you don’t want to use authentication option, you can disable auth on ntp.conf file and disable ntp authentication on switch.

Server stratum number must less than current client stratum number

3 Configuring Phy Loopback

3.1 Overview

Phy loopback is a proprietary based loopback. There are 2 types of phy loopback: phy(including internal and external) level loopback and port level loopback.

If a physical port is configured as “external phy loopback”, all packets coming into this port should be loopback back from the port itself at phy level.

If a physical port is configured as “internal phy loopback”, all packets expected out from this port should be looped back to specified physical port.

If a physical port is configured as “port loopback”, all packets coming into this port should be looped back from the port itself, and whether to swap the SMAC with the DMAC should be selectable by users. And if the MAC is swapped, the CRC should be recalculated.

3.2 Configuring external phy loopback

3.2.1 Topology

This chapter will descript how to configure phy or port level loopback.

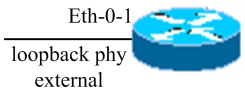

Figure 3-1 External phy topo

3.2.2 Configuration

Switch# configure terminal	Enter the Configure mode.

Switch(config)# interface eth-0-1	Enter the Interface mode.
Switch(config-if)# no shutdown	Configure the port up
Switch(config-if)# loopback phy external	Configure the port as external phy loopback
Switch(config-if)# end	Exit the Interface mode and enter the EXEC mode.
Switch# show phy loopback	Show configuration

3.3 Configuring internal phy loopback

3.3.1 Topology

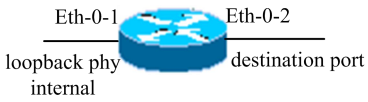

Figure 3-2 Internal phy topo

3.3.2 Configuration

Switch # configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-2	Enter the Interface mode.
Switch(config-if)# no shutdown	Configure the port up
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode.
Switch(config-if)# no shutdown	Configure the port up
Switch(config-if)# loopback phy internal eth-0-2	Configure the port as internal phy loopback, specify interface 2 as the destination port.
Switch(config-if)# end	Exit the Interface mode and enter the EXEC mode.
Switch# show phy loopback	Show configuration

3.4 Configuring port level loopback

3.4.1 Topology

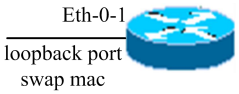

Figure 3-3 Port level loopback topo

3.4.2 Configuration

Switch # configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter the Interface mode.
Switch(config-if)# no shutdown	Configure the port up
Switch(config-if)# loopback port mac-address swap	Configure the port as port level loopback, and enable swapping mac
Switch(config-if)# end	Exit the Interface mode and enter the EXEC mode
Switch# show phy loopback	Show configuration

3.5 Validation

Validate external phy loopback

```
Switch# show phy loopback
 Interface  Type       DestIntf   SwapMac
 -------------------------------------------
 eth-0-1    external   -          -
 -------------------------------------------
```

3.6 Configure L2 ping

3.6.1 Overview

The tool L2 ping is a useful application which's purpose is detecting the connection between two switches. The L2 ping tool is not same with the well-known 'ping IP-ADDRESS' in the WINDOWS system. The normal "ping" is realized by the protocol ICMP which is dependent on the IP layer, so it may be inapplicable if the destination device is only Layer 2 switch. But the protocol used by L2 ping is only relying on Layer 2 ethernet packets.

When L2 ping is started, the L2 ping protocol packet (with ether type '36873(0x9009)') is sent from a specified physical port to another specified destination port. At the destination end, the L2 ping protocol will be sent back via non 802.1ag loopback, or via a configuration "l2 ping response". The device which is pinging, will receive the ping response packet, and print the ping result.

3.6.2 Topology

This chapter will descript how to ping a remote switch's interface mac address.

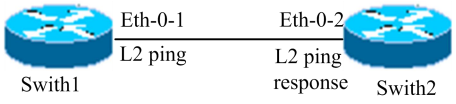

Figure 3-4 L2 pinging a switch port

Configure switch2:

Command	Description
Switch2 # configure terminal	Enter the Configure mode.
Switch2 (config)# interface eth-0-2	Enter the Interface mode.
Switch2 (config-if)# no shutdown	Configure the port up
Switch2 (config-if)# l2 ping response enable	Enable l2 ping response
Switch2 (config-if)# end	Exit the Interface mode and enter the EXEC mode.

Configure switch1:

Command	Description
Switch1# configure terminal	Enter the Configure mode.
Switch1 (config)# interface eth-0-1	Enter the Interface mode.
Switch1 (config-if)# no shutdown	Configure the port up
Switch1 (config-if)# end	Exit the Interface mode and enter the EXEC mode.
Switch1# l2 ping 001e.0808.58f1 interface eth-0-1 count 10 interval 1000 timeout 2000	The mac address can be gained by show interface eth-0-2 on Switch2. User can specify the ping times and interval and timeout time.

3.6.3 Validation

```
Switch1# l2 ping 001e.0808.58f1 interface eth-0-9 count 10 interval 1000 timeout 2000
 Sending 10 L2 ping message(s):

64 bytes from 001e.0808.58f1: sequence = 0, time = 10ms
 64 bytes from 001e.0808.58f1: sequence = 1, time = 15ms
 64 bytes from 001e.0808.58f1: sequence = 2, time = 13ms
 64 bytes from 001e.0808.58f1: sequence = 3, time = 12ms
 64 bytes from 001e.0808.58f1: sequence = 4, time = 20ms
 64 bytes from 001e.0808.58f1: sequence = 5, time = 21ms
 64 bytes from 001e.0808.58f1: sequence = 6, time = 12ms
 64 bytes from 001e.0808.58f1: sequence = 7, time = 16ms
 64 bytes from 001e.0808.58f1: sequence = 8, time = 14ms
 64 bytes from 001e.0808.58f1: sequence = 9, time = 17ms

 L2 ping completed.
 ----------------------------------
 10 packet(s) transmitted, 10 received, 0 % packet loss
```

4 Configuring RMON

4.1 Overview

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switched on all connected LAN segments.

RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

4.2 Topology

Figure 4-1 Rmon1 topo

4.3 Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# rmon collection stats 1 owner test	Create a statistic group on eth-0-1
Switch(config-if)# rmon collection history 1 buckets 100 interval 1000 owner test	Create a history group on interface eth-0-1
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# rmon event 1 log trap public description test_event owner test	Create an event with log and trap both set. Description is “test_event” the owner is test
Switch(config)# rmon alarm 1 etherStatsEntry.6.1 interval 1000 delta rising-threshold 1000 event 1 falling-threshold 1 event 1 owner test	Create a alarm using event 1 we created before and monitor the alarm on ETHERSTATSBROADCASTPKTS on eth-0-1

4.4 Validation

The result of show information about the configured RMON.

```
Switch# show rmon statistics
  Rmon collection index 1
        Statistics ifindex = 1, Owner: test
        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
```

```
Switch# show rmon history
  History index = 1
        Data source ifindex = 1
        Buckets requested = 100
        Buckets granted = 100
        Interval = 1000
        Owner: test
```

```
Switch# show rmon event
  Event Index = 1
        Description: test_event
        Event type Log & Trap
        Event community name: public
        Last Time Sent = 00:00:00
        Owner: test
```

```
Switch# show rmon alarm
  Alarm Index = 1
  Alarm status = VALID
  Alarm Interval = 1000
  Alarm Type is Delta
  Alarm Value = 00
  Alarm Rising Threshold = 1000
  Alarm Rising Event = 1
  Alarm Falling Threshold = 1
  Alarm Falling Event = 1
  Alarm Owner is test
```

5 Configuring SNMP

5.1 Overview

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS). The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent. The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data. An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Error user authentication, restarts, link status (up or down), MAC address tracking, closing of a Transmission Control Protocol (TCP) connection, loss of connection to a neighbor, or other significant events may send a trap.

5.2 References

SNMP module is based on the following RFC draft:

SNMPv1: Defined in RFC 1157.

SNMPv2C: Defined in RFC 1901.

SNMPv3: Defined in RFC 2273 to 2275.

5.3 Terminology

Following is a brief description of terms and concepts used to describe the SNMP protocol:

Agent

A network-management software module, an agent has local knowledge of management information and translates that information into a form compatible with SNMP.

Management Information Base (MIB)

Management Information Base, collection of information is organized hierarchically.

Engine ID

A unique ID for a network's node.

Trap

Used by managed devices to asynchronously report events to the NMS.

5.4 Topology

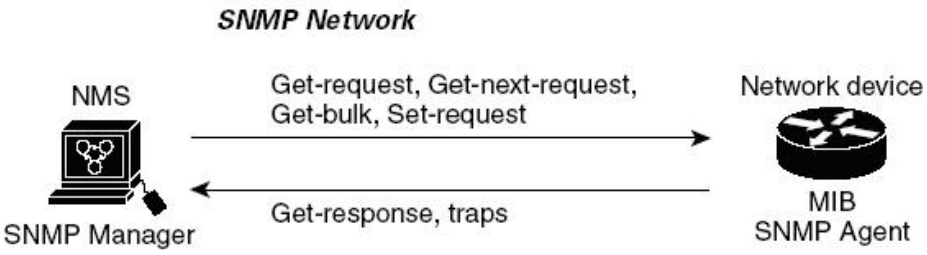

Figure 5-1 SNMP Network

As shown in the figure SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The

SNMP agent also responds to MIB-related queries sent by the SNMP manager in get-request, get-next-request, and set-request format.

5.5 Configuring Enable SNMP

Beginning in privileged EXEC mode, follow these steps to configure a community string on the switch.

5.5.1 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# snmp-server enable	Enable SNMP feature
Switch(config)# end	Return to privileged EXEC mode

5.5.2 Validation

```
Switch# show running-config
snmp-server enable
```

5.6 Configuring community string

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. Optionally, you can specify one or more of these characteristics associated with the string:

- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

Beginning in privileged EXEC mode, follow these steps to configure a community string on the switch.

5.6.1 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# snmp-server view DUT included 1	Configure a view named “DUT”

Switch(config)# snmp-server community public read-only view DUT	Configure a community named “public” with read access and view “DUT”
Switch(config)# end	Return to privileged EXEC mode

5.6.2 Validation

```
Switch# show running-config
snmp-server view DUT included .1
snmp-server community public read-only view DUT
```

5.7 Configuring SNMPv3 Groups, Users and Accesses

You can specify an identification name (engine ID) for the local SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, you can add new users to the SNMP group, and you can add access for the SNMP group.

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the switch.

5.7.1 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# snmp-server engineID 8000123456	Configure a name for local SNMP
Switch(config)# snmp-server usm-user usr1 authentication md5 mypassword privacy des yourpassword	Configure a user “usr1” for local SNMP. Its authentication level is md5 and password is “mypassword”. Its privacy level is des and password is “yourpassword”.
Switch(config)# snmp-server group grp1 user usr1 security-model usm	Configure a group and add the user to the SNMP group
Switch(config)# snmp-server access grp1 security-model usm noauth	Configure a SNMP group’s access
Switch(config)# end	Return to privileged EXEC mode

5.7.2 Validation

```
Switch# show running-config
snmp-server engineID 8000123456
snmp-server usm-user usr1 authentication md5 mypassword privacy des yourpassword
snmp-server group grp1 user usr1 security-model usm
snmp-server access grp1 security-model usm noauth
```

5.8 Configuring SNMPv1 and SNMPv2 notifications

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the switch.

5.8.1 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# snmp-server trap enable all	Enable all supported traps
Switch(config)# snmp-server trap target-address 10.0.0.2 community public	Configure a remote trap manager which IP is “10.0.0.2”
Switch(config)# snmp-server trap target-address 2001:1000::1 community public	Configure a remote trap manager which IPv6 address is “2001:1000::1”
Switch(config)# end	Return to privileged EXEC mode

5.8.2 Validation

```
Switch# show running-config
snmp-server trap target-address 10.0.0.2 community public
snmp-server trap target-address 2001:1000::1 community public
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

5.9 Configuring SNMPv3 notifications

5.9.1 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# snmp-server trap enable all	Enable all supported traps
Switch(config)# snmp-server notify notif1 tag tmptag trap	Configure a trap notify item for SNMPv3
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist tmptag	Configure a remote trap manager’s IP address

Switch(config)# snmp-server target-address t1 param p1 2001:1000::1 taglist tag1	Configure a remote trap manager's IPv6 address
Switch(config)# snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth	Add a local user to SNMPv3 notifications
Switch(config)# end	Return to privileged EXEC mode

5.9.2 Validation

```
Switch# show snmp-server trap-receiver
snmp-server notify notif1 tag tmptag trap
snmp-server target-address t1 param p1  2001:1000::1 taglist tag1
snmp-server target-address targ1 param parm1  10.0.0.2 taglist tmptag
snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

6 Configuring SFLOW

6.1 Overview

sFlow is a technology for monitoring traffic in data networks containing switches and routers. In particular, it defines the sampling mechanisms implemented in a sFlow Agent for monitoring traffic, and the format of sample data used by the sFlow Agent when forwarding data to a central data collector.

The architecture and sampling techniques used in the sFlow monitoring system are designed to provide continuous site-wide (and network-wide) traffic monitoring for high speed switched and routed networks.

The sFlow Agent uses two forms of sampling: statistical packet-based sampling of switched flows, and time-based sampling of network interface statistics.

6.2 Terminology

Sflow: Sampled flow

6.3 Topology

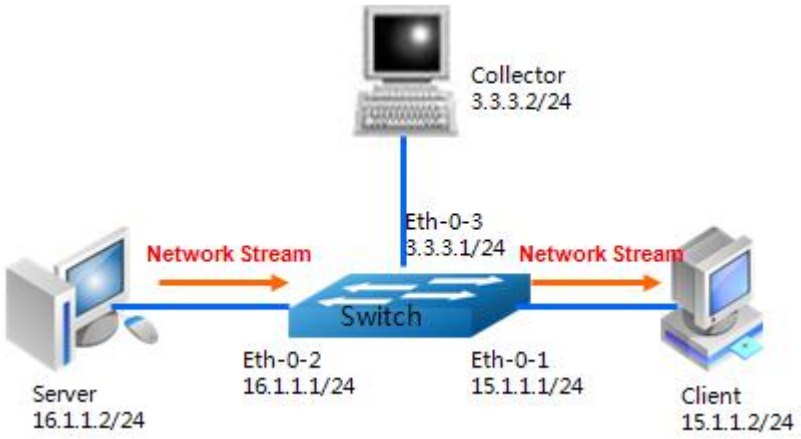

Figure 6-1 Sflow topology

6.4 Configurations

Default Configuration

Feature	Default Setting
global sflow	disabled
sflow on port	disable
collector udp port	6343
counter interval time	20 seconds

Sflow Configuration

This example shows the configuration required for enable sampled flow. All packets ongoing ingress interface eth-0-1 will be sampled with a specified rate, and then the sample packets will be sent to collocter 3.3.3.2 for analysis.

Switch# configure terminal	Enter the Configure mode
Switch(config)# sflow enable	Enable sFlow globally

Switch(config)# sflow counter interval 20	Set sFlow polling-interval for counter sample
Switch(config)# sflow agent ip 3.3.3.1	Set sFlow agent
Switch(config)# sflow collector 3.3.3.2 6342	Set sFlow collector
Switch(config)# sflow collector 2001:1000::1	Set sFlow collector
Switch(config)# interface eth-0-1	Enter the interface mode
Switch(config-if)# sflow flow-sampling rate 8192	Set flow sampling rate
Switch(config-if)# sflow flow-sampling enable input	Enable packet sampling
Switch(config-if)# sflow counter-sampling enable	Enable packet counter
Switch(config-if)# no switchport	Change to router port
Switch(config-if)# ip address 15.1.1.1/24	Set ip address on this port
Switch(config-if)# exit	Exit to config mode
Switch(config)# interface eth-0-2	Enter the interface mode
Switch(config-if)# no switchport	Change to router port
Switch(config-if)# ip address 16.1.1.1/24	Set ip address on this port
Switch(config-if)# exit	Exit to config mode
Switch(config)# interface eth-0-3	Enter the interface mode
Switch(config-if)# no switchport	Change to router port
Switch(config-if)# ip address 3.1.1.1/24	Set ip address on this port

6.5 Validation

To display the sflow configuration, use following privileged EXEC command.

```
Switch# show sflow
sFlow Global Information:
 Agent IP address              : 2.2.2.1
 Agent IPv6 address            : 2026::2
 Counter Sampling Interval     : 20 seconds
 Collector 1:
  Address: 3.3.3.2
  Port: 6342
 Collector 2:
```

```
  Address: 2001:1000::1
  Port: 6343

sFlow Port Information:
                                      Flow-Sample         Flow-Sample
 Port         Counter     Flow        Direction     Rate
 ---------------------------------------------------------
 eth-0-1      Enable      Enable      Input         8192
```

7 Configuring LLDP

1.1 Overview

LLDP（Link Layer Discovery Protocol）is the discovery protocol on link layer defined as standard in IEEE 802.1ab. Discovery on Layer 2 can locate interfaces attached to the devices exactly with connection information on layer 2,such as VLAN attribute of port and protocols supported, and present paths among client, switch, router , application servers and other network servers. These detailed description is helpful to get useful information for diagnosing network fast, like topology of devices attached, conflict configuration between devices, reason of network failure.

1.2 Terminology

LLDP： Link Layer Discovery Protocol

1.3 Topology

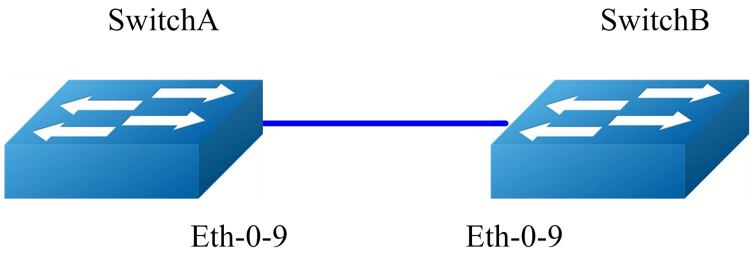

Figure 1-1 LLDP topology

1.4 Configurations

Basic Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# lldp enable	Enable LLDP globally
Switch(config)# interface eth-0-9	Enter the interface mode
Switch(config)# no shutdown	Up the interface
Switch(config-if)# no lldp tlv 8021-org-specific vlan-name	Cancel the selection of Vlan Name TLV in IEEE 802.1 tlv set
Switch(config-if)# lldp tlv med location-id ecs-elin 1234567890	Select and configure the Location ID TLV in MED tlv set
Switch(config-if)# lldp enable txrx	Enable LLDP with TXRX mode on port

State Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# lldp timer msg-tx-interval 40	Configure the transmitting interval of LLDP packet to 40 seconds
Switch(config)# lldp timer tx-delay 3	Configure the transmitting delay of LLDP packet to 3 seconds
Switch(config)# lldp timer reinitDelay 1	Configure the reinit delay of LLDP function to 1 second

1.5 Validation

To display the LLDP configuration, use following privileged EXEC command.

```
Switch# show lldp local config
LLDP global configuration:
============================================================
LLDP function global enabled : YES
LLDP msgTxHold     : 4
LLDP msgTxInterval : 40
LLDP reinitDelay   : 1
LLDP txDelay       : 3
```

```
Switch# show lldp local config interface eth-0-9
LLDP configuration on interface eth-0-9 :
============================================================
```

```
LLDP admin status : TXRX

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
    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
    Location Identification TLV
    Extended Power-via-MDI TLV
    Inventory TLV
```

```
Switch# show running-config
!
lldp enable
lldp timer msg-tx-interval 40
lldp timer reinit-delay 1
lldp timer tx-delay 3

。。。
interface eth-0-9
lldp enable txrx
 no lldp tlv 8021-org-specific vlan-name
 lldp tlv med location-id ecs-elin 1234567890
!
```

```
Switch# show lldp neighbor
Remote LLDP Information
============================================================
Chassis ID type: Mac address
Chassis ID     : 48:16:be:a4:d7:09
Port ID type   : Interface Name
Port ID        : eth-0-9

TTL : 160
Expired time: 134
```

```
…
Location Identification :
    ECS ELIN: 1234567890
```

8 Configuring IPFIX

8.1 Overview

Traffic on a data network can be seen as consisting of flows passing through network elements. For administrative or other purposes, it is often interesting, useful, or even necessary to have access to information about these flows that pass through the network elements. This requires uniformity in the method of representing the flow information and the means of communicating the flows from the network elements to the collection point. This is what IPFIX can do.

Before IPFIX was introduced, there is a Cisco private method NetFlow. IPFIX is similar to NetFlow and is based on NetFlow version 9.

8.2 Configurations

This example shows the minimum configuration required for enabling IPFIX on a switch.

SwitchA# configure terminal	Enter the Configure mode
Switch(config)# ipfix global flow aging 300	Configure the timeout to be 300 seconds of ipfix flow
SwitchA(config)# ipfix recorder recorder1	Enter the recorder mode,create a recorder1
Switch(Config-ipfix-reocrder)# match mac source address	Configure to use source mac address to distinguish flow s
Switch(Config-ipfix-reocrder)# match ipv4 source address mask 32	Configure to use source IPV4 address to distinguish flows
Switch(Config-ipfix-reocrder)# match ipv4 destination address mask 32	Configure to use destination IPV4 address to distinguish flows

Switch(Config-ipfix-reocrder)# match vxlan-vni	Configure to use vxlan-vni to distinguish flows
Switch(Config-ipfix-reocrder)# collect counter bytes	Configure to collect the byte number of flows
Switch(Config-ipfix-reocrder)# collect counter packets	Configure to collect the packet number of flows
Switch(Config-ipfix-reocrder)# exit	Exit the ipfix recoeder mode
Switch(config)# ipfix sampler sampler1	Enter the sampler mode,create a sampler1
Switch(Config-ipfix-sampler)# 1 out-of 100	Configure the sampling rate of the ipfix sampler is 100
Switch(Config-ipfix- sampler)# exit	Exit ipfix sampler mode
Switch(config)# ipfix exporter exporter1	Enter exporter mode,create a exporter1
Switch(Config-ipfix-exporter)# destination HOST	Configure the collecter host that need to receive the flow records
Switch(Config-ipfix-exporter)# source interface eth-0-2	Configure to use interface eth-0-2 to send flow records to the collecter
Switch(Config-ipfix-exporter)# flow data timeout 200	Configure to send flow records to the collecter every 200 seconds
Switch(Config-ipfix-exporter)# event flow end timeout	Configure to send flow records to the collecter immediately when the flow records is timeout
Switch(Config-ipfix-exporter)# exit	Exit ipfix exporter mode
Switch (config)# ipfix monitor monitor1	Enter monitor mode,create a monitor1
Switch (Config-ipfix-monitor)# recorder recorder1	Configure recorder
Switch (Config-ipfix-monitor)# exporter exporter1	Configure exporter
Switch (Config-ipfix-monitor)# exit	Exit ipfix monitor mode
Switch(config)# interface eth-0-1	Enter interface mode

Switch(config-if)# ipfix monitor monitor1 sampler sampler1 packet input	Configure to enable ipfix in ingress on the interface eth-0-1 for all packets by using monitor1 and sampler1, configure to use inner header's fields that matched to distinguish flows
Switch(config-if)# exit	Exit interface mode

8.3 Validation

Use the commands as follows to validate the configuration:

Switch A output

```
Switch# show ipfix global
IPFIX global informaition:
     Current flow cache number            : 0(ingress: 0, egress: 0)
     Flow cache aging interval             : 300 seconds
     Flow cache sampler mode             : all flow
```

```
Switch# show ipfix recorder recorder1
IPFIX recorder informaition:
    Name        : recorder1
    Description   :
    Match info   :
        match Source Mac Address
        match IPv4 Source Address
        match IPv4 Destination Address
        match Vxlanvni
    Collect info   :
        collect Flow Byte Number
        match Flow Packet Number
```

```
Switch# show ipfix exporter exporter1
IPFIX exporter informaition:
    Name                          : exporter1
    Description                    :
    Exporter Interface               : eth-0-2
    Collector Name                  : HOST
    IPFIX message protocol           : UDP
    IPFIX message destination Port      : 3000
    IPFIX message TTL value          : 255
    IPFIX message DSCP value         : 63
    IPFIX data interval               : 200
    IPFIX template interval            : 1800
```

```
    IPFIX exporter events              :
        Flow aging event
```

```
Switch# show ipfix sampler sampler1
IPFIX sampler informaition:
    Name                          : sampler1
    Description                     :
    Rate                           : 100
```

```
Switch# show ipfix monitor monitor1
IPFIX monitor informaition:
    Name                           : monitor1
    Description                      :
    Recorder                        : recorder1
    exporter                         : exporter1
```