

FSOS

Device Management Configuration Guide

Contents

1 Configuring STM.....	8
1.1 Overview.....	8
1.2 Configuration.....	9
1.3 Validation.....	9
2 Configuring Syslog.....	11
2.1 Overview.....	11
2.2 Terminology.....	11
2.3 Configuring Logging State.....	13
2.3.1 Topology.....	13
2.3.2 Configurations.....	13
2.3.3 Validation.....	13
2.4 Configuring Logging Buffer Size.....	14
2.4.1 Configurations.....	14
2.4.2 Validation.....	14
3 Configuring Mirror.....	16
3.1 Overview.....	16
3.2 Terminology.....	16
3.3 Topology.....	19
3.4 Configuration.....	20
3.5 Validation.....	20
4 Configuring Multi-destination Mirror.....	22
4.1 Overview.....	22
4.2 Terminology.....	22
4.3 Topology.....	25

4.4 Configuration.....	25
4.5 Validation.....	26
5 Configuring Remote Mirror.....	28
5.1 Configuring Remote Mirror.....	28
5.1.1 Overview.....	28
5.1.2 Terminology.....	28
5.1.3 Topology.....	29
5.1.4 Configuration.....	30
5.1.5 Validation.....	33
5.2 Configuring Mac Escape for Remote Mirror.....	34
5.2.1 Overview.....	34
5.2.2 Topology.....	35
5.2.3 Configuration.....	35
5.2.4 Validation.....	36
6 Configuring Device Management.....	37
6.1 Overview.....	37
6.2 Configuring console port for management.....	37
6.2.1 Configuration.....	37
6.2.2 Validation.....	38
6.3 Configuring out band Ethernet port for management.....	38
6.3.1 Configuration.....	38
6.3.2 Validation.....	38
6.4 Configuring Temperature.....	39
6.4.1 Configuring temperature threshold.....	39
6.4.2 Validation.....	39
6.5 Configuring Fan.....	40
6.5.1 Configuration.....	40
6.5.2 Validation.....	40
6.6 Configuring Power.....	41

6.6.1 Configuration.....	41
6.6.2 Validation.....	41
6.7 Configuring Transceiver.....	41
6.7.1 Configuration.....	42
6.7.2 Validation.....	42
6.8 Upgrade bootrom.....	43
6.8.1 Configurations.....	43
6.8.2 Validation.....	43
6.9 Upgrade EPLD.....	44
6.9.1 Configurations.....	44
6.9.2 Validation.....	44
7 Configuring Bootrom.....	45
7.1 Overview.....	45
7.2 Configuring Boot from TFTP Server.....	45
7.2.1 Configurations.....	45
7.2.2 Validation.....	46
7.3 Configuring Boot from Flash.....	46
7.3.1 Configurations.....	46
7.3.2 Validation.....	47
7.4 Set boot IP.....	48
7.4.1 Configurations.....	48
7.4.2 Validation.....	48
7.5 Upgrade bootrom.....	49
7.5.1 Configurations.....	49
7.5.2 Validation.....	49
7.6 Set gateway IP.....	49
7.6.1 Configurations.....	49
7.6.2 Validation.....	50
8 Configuring Bootup Diagnostic.....	51

8.1 Overview.....	51
8.2 Configuration.....	51
8.3 Validation.....	51
9 Configuring PoE.....	53
9.1 Overview.....	53
9.2 Terminology.....	54
9.3 Topology.....	55
9.4 Configuration.....	55
9.5 Validation.....	57
10 Configuring SmartConfig.....	59
10.1 Overview.....	59
10.2 Topology.....	61
10.3 Configuration.....	61
10.4 4 boot or reboot. Validation.....	62
11 Configuring Stacking.....	63
11.1 Overview.....	63
11.2 Topology.....	63
11.3 Configuration.....	64
11.4 Validation.....	65
11.5 Warning.....	66
11.6 Remove Stacking.....	66
12 Reboot Logs.....	67
12.1 Overview.....	67
12.2 Validation.....	67
12.3 Warning.....	68

Tables

Table 2-1 System Message Log Facility Types.....	12
Table 2-2 Severity Level Definitions.....	12

Figures

Figure 2-1 NTP server-client with authentication topology.....	13
Figure 2-2 Log information on syslog Servers.....	15
Figure 3-1 Mirror.....	19
Figure 4-1 Multi-destination Mirror.....	25
Figure 5-1 Remote Mirror.....	29
Figure 5-2 Mac Escape.....	35
Figure 10-1 PoE Topology.....	55
Figure 11-1 SmartConfig Topology.....	61
Figure 12-1 Stacking Topology.....	63

1 Configuring STM


1.1 Overview

Switch Table Management (STM) is used to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network.

You can select a profile to provide maximum system usage for some functions; for example, use the default profile to balance resources and use vlan profile to obtain max MAC entries.

To allocate ternary content addressable memory (TCAM) resources for different usages, the switch STM profile prioritize system resources to optimize support for certain features. You can select STM templates to optimize these features:

- **ipv4**—The routing template maximizes system resources for unicast routing, typically required for a router or aggregator in the center of a network.
- **vlan**—The VLAN template supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.
- **default**—The default template gives balance to all functions.
- **ipv6**- The dual IPv4 and IPv6 templates allow the switch to be used in dual stack environments (supporting both IPv4 and IPv6). Using the dual stack templates results in less TCAM capacity allowed for each resource. Do not use them if you plan to forward

only IPv4 traffic.  **NOTE**

When users configured a profile mode which is not exist in the next reboot image, then default hardware configure will be used when system up with the next image. The hardware configure may be different from the default profile.

1.2 Configuration

Follow these guidelines when selecting and configuring STM profiles.

- You must reload the switch for the configuration to take effect.
- Use the `stm prefer vlan` global configuration command only on switches intended for Layer 2 switching with no routing.
- Do not use the `ipv4` profile if you do not have routing enabled on your switch. The `stm prefer ipv4` global configuration command prevents other features from using the memory allocated to IPv4 unicast routing in the routing profile.

Switch# configure terminal	Enter configuration mode
Switch(config)# stm prefer ipv4	Select ipv4 profile for best supporting IP unicast routing
Switch(config)# end	Return to the EXEC mode
Switch# reload	Reload system

1.3 Validation

This is an example of an output display for default template.

Switch# show stm prefer

```
Current profile is :default
The selected profile optimizes the resources in
the switch to make balance entry number among
route, mac related tables.

number of Ethernet features:
  VLAN number                : 4094
  VLAN forwarding instances   : 4094
  Ucast MAC addresses         : 32768
  Mcast MAC addresses         : 2048
  Blackhole MAC addresses     : 64
  Max applied VLAN mapping    : 1024
number of OAM features:
  BFD sessions                : 128
  CFM local&remote MEPS       : 1000
  CFM Ethernet Locked Signal   : 48
```

G.8031 groups	: 64
G.8032 rings	: 32
number of VLAN class rules:	
MAC based VLAN classification	: 256
IPv4 based VLAN classification	: 512
IPv6 based VLAN classification	: 256
number of Dot1x Mac entry:	
DOT1X MAC BASED	: 256
number of IP unicast routing:	
IPv4 host routes	: 3072
Indirect IPv4 routes	: 6144
IPv4 ECMP groups	: 16
IPv4 policy based routes	: 32
IPv6 host routes	: 1024
Indirect IPv6 routes	: 2048
IPv6 ECMP groups	: 14
IP Tunnel Peers	: 8
number of IP multicast routing:	
IPv4 Mcast routes	: 511
IPv4 Mcast total members	: 2044
IPv6 Mcast routes	: 127
IPv6 Mcast total members	: 508
number of Security features:	
IPv4 source guard entries	: 1024
IPv4 ACL/QOS flow entries	: 863
IPv6 ACL/QOS flow entries	: 127

The profile stored for use after the next reload is the ipv4 profile.

number of Ethernet features:	
VLAN number	: 4094
VLAN forwarding instances	: 4094
Ucast MAC addresses	: 32768
Mcast MAC addresses	: 1024
Blackhole MAC addresses	: 64
Max applied VLAN mapping	: 1536
number of VLAN class rules:	
MAC based VLAN classification	: 256
IPv4 based VLAN classification	: 512
number of Dot1x Mac entry:	
DOT1X MAC BASED	: 256
number of IP unicast routing:	
IPv4 host routes	: 6144
Indirect IPv4 routes	: 12288
IPv4 ECMP groups	: 30
IPv4 policy based routes	: 64
number of IP multicast routing:	
IPv4 Mcast routes	: 511
IPv4 Mcast total members	: 2044
number of Security features:	
IPv4 source guard entries	: 512
IPv4 ACL/QOS flow entries	: 1535

2

Configuring Syslog

This document is intended to give a usage example for system log feature.

2.1 Overview

The system message logging software can save messages in a log file or direct the messages to other devices. The system message logging facility has these features:

- Provides you with logging information for monitoring and troubleshooting.
- Allows you to select the types of logging information that is captured.
- Allows you to select the destination of the captured logging information.

By default, the switch logs normal but significant system messages to its internal buffer and sends these messages to the system console. You can specify which system messages should be saved based on the type of the severity level. The messages are time-stamped to enhance real-time debugging and management.

You can access the logged system messages using the switch command-line interface (CLI) or by saving them to a properly configured log server. The switch software saves the log messages in an internal buffer that can store up to 1000 messages. You can monitor the system messages remotely by accessing the switch through Telnet or the console port, or by viewing the logs on a log server.

2.2 Terminology

Logging: Current logging configuration

Show: Show logging configuration

Levels: Severity level information

Enable: Enable write log to local file

Disable: Disable write log to local file

Table 2-1 System Message Log Facility Types

Facility Name	Definition
kern	kernel messages
user	random user-level messages
mail	mail system
daemon	system daemons
auth	security/authorization messages
syslog	messages generated internally by syslogd
lpr	line printer subsystem
news	network news subsystem
uucp	UUCP subsystem
cron	clock daemon
authpriv	security/authorization messages (private)
ftp	ftp daemon

Table 2-2 Severity Level Definitions

Severity Level	Definition
emergency	system is unusable
alert	action must be taken immediately
critical	critical conditions
error	error conditions
warning	warning conditions
notice	normal but significant condition
information	Informational

Severity Level	Definition
debug	debug-level messages

2.3 Configuring Logging State

2.3.1 Topology



Figure 2-2 NTP server-client with authentication topology

2.3.2 Configurations

Switch# configure terminal	Enter the Configure mode.
Switch(config)# logging server enable	Enable the logging state for a Telnet session
Switch(config)# logging server address 1.1.1.1	Specify the IPv4 address of one log servers
Switch(config)# logging server address 2001:1000::2	Specify the IPv6 address of one log servers
Switch(config)# logging server severity debug	Set the severity levels for slog server messages
Switch(config)# logging server facility mail	Set the facility for log server messages

2.3.3 Validation

And you can check the result by using show logging command:

```
Switch# show logging
```

```
Current logging configuration:
=====
logging buffer 500
logging timestamp bsd
logging file enable
logging level file warning
logging level module debug
logging server enable
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging server address 2001:1000::2
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```

2.4 Configuring Logging Buffer Size

By default, the number of messages to log to the logging buffer is 500. If desired, you can set the number between 10 and 1000.

2.4.1 Configurations

Switch# configure terminal	Enter the Configure mode
Switch(config)# logging buffer 700	Set the number of messages to log to the logging buffer

2.4.2 Validation

And you can check the result by using show logging command.

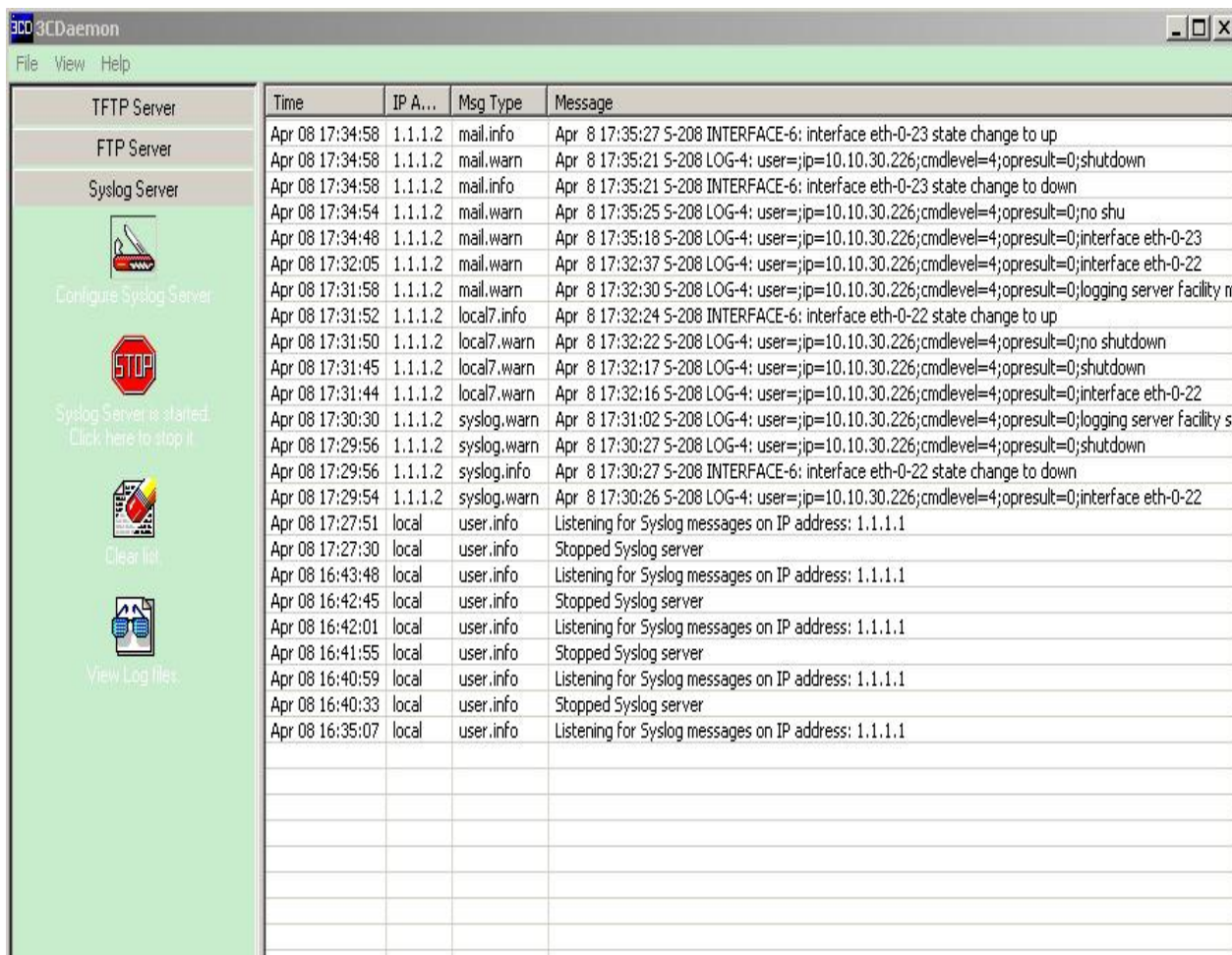
Switch# show logging

```
Current logging configuration:
=====
logging buffer 700
logging timestamp bsd
logging file enable
logging level file warning
logging level module debug
logging server enable
```

```
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```



You can use command to check showing Logging Information. When configuring the syslog Servers, make sure the cables is linked correctly and two computers can ping each other. Before you can send the system log messages to a log server, you must configure Syslog Software, at the end you can see the log from your software.



	Time	IP A...	Msg Type	Message
TFTP Server	Apr 08 17:34:58	1.1.1.2	mail.info	Apr 8 17:35:27 S-208 INTERFACE-6: interface eth-0-23 state change to up
FTP Server	Apr 08 17:34:58	1.1.1.2	mail.warn	Apr 8 17:35:21 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;shutdown
Syslog Server	Apr 08 17:34:58	1.1.1.2	mail.info	Apr 8 17:35:21 S-208 INTERFACE-6: interface eth-0-23 state change to down
	Apr 08 17:34:54	1.1.1.2	mail.warn	Apr 8 17:35:25 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;no shu
	Apr 08 17:34:48	1.1.1.2	mail.warn	Apr 8 17:35:18 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;interface eth-0-23
	Apr 08 17:32:05	1.1.1.2	mail.warn	Apr 8 17:32:37 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;interface eth-0-22
	Apr 08 17:31:58	1.1.1.2	mail.warn	Apr 8 17:32:30 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;logging server facility m
	Apr 08 17:31:52	1.1.1.2	local7.info	Apr 8 17:32:24 S-208 INTERFACE-6: interface eth-0-22 state change to up
	Apr 08 17:31:50	1.1.1.2	local7.warn	Apr 8 17:32:22 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;no shutdown
	Apr 08 17:31:45	1.1.1.2	local7.warn	Apr 8 17:32:17 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;shutdown
	Apr 08 17:31:44	1.1.1.2	local7.warn	Apr 8 17:32:16 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;interface eth-0-22
	Apr 08 17:30:30	1.1.1.2	syslog.warn	Apr 8 17:31:02 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;logging server facility s;
	Apr 08 17:29:56	1.1.1.2	syslog.warn	Apr 8 17:30:27 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;shutdown
	Apr 08 17:29:56	1.1.1.2	syslog.info	Apr 8 17:30:27 S-208 INTERFACE-6: interface eth-0-22 state change to down
	Apr 08 17:29:54	1.1.1.2	syslog.warn	Apr 8 17:30:26 S-208 LOG-4: user=;ip=10.10.30.226;cmdlevel=4;opresult=0;interface eth-0-22
	Apr 08 17:27:51	local	user.info	Listening for Syslog messages on IP address: 1.1.1.1
	Apr 08 17:27:30	local	user.info	Stopped Syslog server
	Apr 08 16:43:48	local	user.info	Listening for Syslog messages on IP address: 1.1.1.1
	Apr 08 16:42:45	local	user.info	Stopped Syslog server
	Apr 08 16:42:01	local	user.info	Listening for Syslog messages on IP address: 1.1.1.1
	Apr 08 16:41:55	local	user.info	Stopped Syslog server
	Apr 08 16:40:59	local	user.info	Listening for Syslog messages on IP address: 1.1.1.1
	Apr 08 16:40:33	local	user.info	Stopped Syslog server
	Apr 08 16:35:07	local	user.info	Listening for Syslog messages on IP address: 1.1.1.1

Figure 2-3 Log information on syslog Servers

3

Configuring Mirror

3.1 Overview

You can analyze network traffic passing through ports or vlans by using mirror function to send a copy of the traffic to another port on the switch that has been connected to a Switch Probe device or other Remote Monitoring (RMON) probe or security device. Mirrors received or sent (or both) traffic on a source port and received traffic on one or more source ports or source vlans, to a destination port for analysis.

Only traffic that enters or leaves source ports or traffic that enters source vlans can be monitored by using mirror; traffic that gets routed to ingress source ports or source vlans cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another vlans to the source vlans is not monitored; however, traffic that is received on the source vlan and routed to another vlan is monitored.

Mirror does not affect the switching of network traffic on source ports or source vlans; a copy of the packets received or sent by the source interfaces are sent to the destination interface.

3.2 Terminology

The following describes concepts and terminology associated with mirror configuration.

Mirror Session

A mirror session is an association of a destination port with source ports and source VLANs. You configure mirror sessions by using parameters that specify the source of network traffic to monitor. Both switched and routed ports can be configured as mirror sources and destinations. You can configure up to 3 mirror sessions.

Mirror sessions do not interfere with the normal operation of the switch. However, an oversubscribed mirror destination, for example, a 10-Mbps port monitoring a 100-Mbps port, results in dropped or lost packets.

You can configure mirror sessions on disabled ports; however, a mirror session does not become active unless you enable the destination port and at least one source port or VLAN for that session.

A mirror session remains inactive after system power-on until the destination port is operational.

Traffic Types

Mirror sessions include these traffic types:

Receive (RX) mirror: The goal of receive (or ingress) mirror is to monitor as much as possible packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received (except these packets: BPDU, LACPDU, BMGPDU, packets have been discarded by IP-MAC binding check for Vlan_based mirror, CRC error packets for both Port_based and vlan_based mirror) by the source is sent to the destination port for that mirror session. You can monitor a series or range of ingress ports or VLANs in a mirror session. Packets that are modified because of routing are copied without modification; that is, the original packet is copied. Packets that are modified because of quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied with modification. Packets that are modified because of VLAN translation or VLAN classification is copied with the modification. Some features that can cause a packet to be dropped during receive processing have no effect on mirror, the destination port can receive a copy of the packet even if the actual incoming packet is dropped. These features include ingress ACL, VLAN's ingress filter, MAC filter, STP, VLAN tag control, port security, unknown routing packets.

Transmit (TX) mirror: The goal of transmit (or egress) mirror is to monitor as much as possible packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet (except these packets: packets from CPU port for Vlan_based mirror, mirroring packets for both Port_based and vlan_based mirror) sent by the source is

sent to the destination port for that mirror session. Some features that can cause a packet to be dropped during transmit processing might have affect on mirror.

Both: In a mirror session, you can monitor a single port for both received and sent packets.

Source Port

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis. In a single mirror session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs (up to the maximum number of VLANs supported).

A source port has these characteristics:

It can be any port type (for example, EtherChannel).

It can only be monitored in a single mirror session.

It cannot be a destination port.

Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction would apply to all the physical ports in the group.

Source ports can be in the same or different VLANs.

For VLAN sources, user should create VLAN Interface before configure a vlan source.

It can not be a physical port that is assigned to an EtherChannel group.

Destination Port

Each mirror session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports and VLANs.

The destination port has these characteristics:

It must reside on the same switch as the source port.

It can be any Ethernet physical port.

It can not be physical port that is assigned to an EtherChannel group.

It can participate in only one mirror session at a time (a destination port in one mirror session cannot be a destination port for a second mirror session).

It cannot be a source port.

The port does not transmit any traffic except that required for the mirror session.

It does not participate in spanning tree while the mirror session is active.

When it is a destination port, all other normal system function of this port should not work until mirror destination configure disabled on this port.

No address learning occurs on the destination port.

The real statues of the speed/duplex might not coincide with the values which are displayed.

3.3 Topology

For example, in the below figure, all traffic on port 1(the source port) is mirrored to port 2(the destination port). A network analyzer on port 2 receives all network traffic from port 1 without being physically attached to port 1

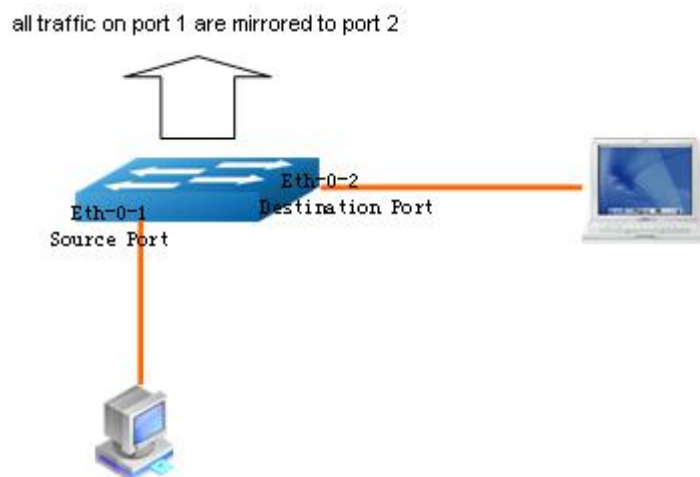


Figure 3-1 Mirror

3.4 Configuration

Mirror's configuration is as follow

Switch# configure terminal	Enter the Configure mode.
Switch(config)# vlan database	Enter the VLAN configure mode
Switch(config-vlan)# vlan 10	Create VLAN 10;
Switch(config-vlan)# exit	Exit the Vlan database mode and enter the Configure mode
Switch(config)# interface vlan10	Create vlan interface and enter the Interface mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface eth-0-2	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface which is prepared to be the destination port
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# monitor session 1 destination interface eth-0-2	Specify the mirror session and the destination port (monitoring port)
Switch(config)# monitor session 1 source interface eth-0-1 both	Specify the mirror session and the source port (monitored port)
Switch(config)# monitor session 1 source vlan 10 rx	Specify the mirror session and the source VLAN
Switch(config)# end	Return to the EXEC mode
Switch# show monitor session 1	Display the session configuration

3.5 Validation

This example shows how to set up a mirror session, session 1, for monitoring source port traffic to a destination port. You can use show monitor session to see the configuration.

Switch # show monitor session 1

```
Session 1
-----
Status      : Valid
Type        : Local Session
Source Ports :
  Receive Only :
  Transmit Only :
  Both         : eth-0-1
Source VLANs :
  Receive Only : 10
  Transmit Only :
  Both         :
Destination Port : eth-0-2
```

4

Configuring Multi-destination Mirror

4.1 Overview

You can analyze network traffic passing through ports by using mirror function to send several copies of the traffic to another port on the switch that has been connected to a Switch Probe device or security device. Mirrors received or sent (or both) traffic on a source port and received traffic on one or more source port, to several destination ports for analysis.

4.2 Terminology

The following describes concepts and terminology associated with mirror configuration.

Mirror Session

A multi-destination mirror session is an association of a destination port with source ports. You configure mirror sessions by using parameters that specify the source of network traffic to monitor. Both switched and routed ports can be configured as mirror sources and destinations. You can configure up to 1 multi-destination mirror sessions.

Mirror sessions do not interfere with the normal operation of the switch. However, an oversubscribed mirror destination, for example, a 10-Mbps port monitoring a 100-Mbps port, results in dropped or lost packets.

You can configure mirror sessions on disabled ports; however, a mirror session does not become active unless you enable the destination port and at least one source port for that session.

A mirror session remains inactive after system power-on until the destination port is operational.

Traffic Types

Mirror sessions include these traffic types:

Receive (RX) mirror: The goal of receive (or ingress) mirror is to monitor as much as possible packets received by the source interface before any modification or processing is performed by the switch. A copy of each packet received (except these packets: BPDU, LACPDU, BMGPDU, packets have been discarded by IP-MAC binding check for Vlan_based mirror, CRC error packets for both Port_based and vlan_based mirror) by the source is sent to the destination port for that mirror session. You can monitor a series or range of ingress ports or VLANs in a mirror session. Packets that are modified because of routing are copied without modification; that is, the original packet is copied. Packets that are modified because of quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied with modification. Packets that are modified because of VLAN translation or VLAN classification is copied with the modification. Some features that can cause a packet to be dropped during receive processing have no effect on mirror, the destination port can receive a copy of the packet even if the actual incoming packet is dropped. These features include ingress ACL, VLAN's ingress filter, MAC filter, STP, VLAN tag control, port security, unknown routing packets.

Transmit (TX) mirror: The goal of transmit (or egress) mirror is to monitor as much as possible packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet (except these packets: packets from CPU port for Vlan_based mirror, mirroring packets for both Port_based and vlan_based mirror) sent by the source is sent to the destination port for that mirror session. Some features that can cause a packet to be dropped during transmit processing might have affect on mirror.

Both: In a mirror session, you can monitor a single port for both received and sent packets.

Source Port

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis. In a single mirror session, you can monitor source port traffic such as

received (Rx), transmitted (Tx), or bidirectional (both). The multi-destination mirror only supports any number of source ports (up to the maximum number of available ports on the switch).

A source port has these characteristics:

It can be any port type (for example, EtherChannel).

It can only be monitored in a single mirror session.

It cannot be a destination port.

Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction would apply to all the physical ports in the group.

It can not be a physical port that is assigned to an EtherChannel group.

Destination Port

A multi-destination mirror session can have several destination ports (also called a monitoring port) that receives a copy of traffic from the source ports.

The destination port has these characteristics:

It must reside on the same switch as the source port.

It can be any Ethernet physical port.

It can not be physical port that is assigned to an EtherChannel group.

It can participate in only one mirror session at a time (a destination port in one mirror session cannot be a destination port for a second mirror session).

It cannot be a source port.

The port does not transmit any traffic except that required for the mirror session.

It does not participate in spanning tree while the mirror session is active.

When it is a destination port, all other normal system function of this port should not work until mirror destination configure disabled on this port.

No address learning occurs on the destination port.

The real statues of the speed/duplex might not coincide with the values which are displayed.

4.3 Topology

For example, in [figure 4-1](#), all traffic on port 1(the source port) is mirrored to port 2 and port 3(the destination port). A network analyzer on port 2 and port 3 receives all network traffic from port 1 without being physically attached to port 1

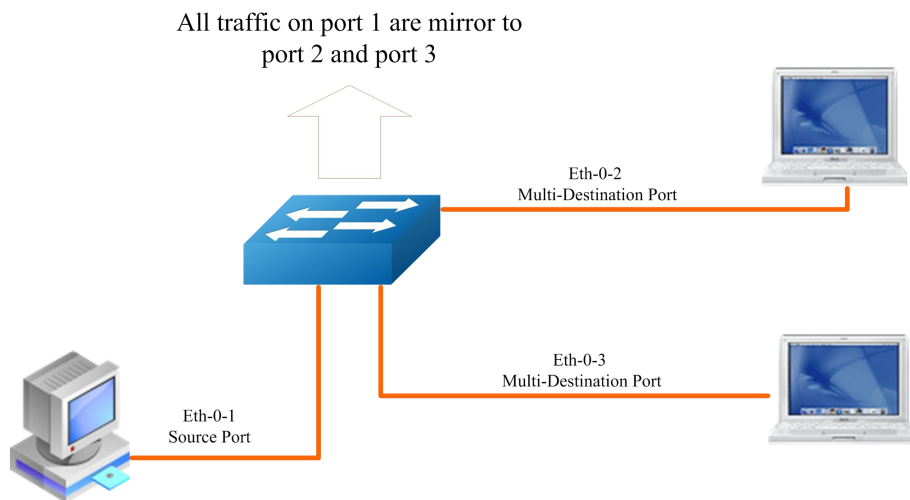


Figure 4-1 Multi-destination Mirror

4.4 Configuration

Mirror's configuration is as follow

Switch# configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface which is prepared to be the destination port.

Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# interface eth-0-2	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface which is prepared to be the destination port.
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# interface eth-0-3	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface which is prepared to be the destination port.
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# monitor session 1 source interface eth-0-1	Specify the mirror session and the source port.
Switch(config)# monitor session 1 destination group 1	Specify the mirror session and the multi destination group.
Switch(config-monitor-d-group)# member eth-0-2	Add interface eth-0-2 to multi destination group
Switch(config-monitor-d-group)# member eth-0-3	Add interface eth-0-3 to multi destination group
Switch(config)# end	Return to the EXEC mode
Switch# show monitor session 1	Display the session configuration.

4.5 Validation

This example shows how to set up a mirror session, session 1, for monitoring source port traffic to a destination port. You can use show monitor session to see the configuration.

Switch# show monitor session 1

```

Session 1
-----
Status      : Valid
Type        : Local Session
Source Ports :
Receive Only :

```

```
Transmit Only :  
Both : eth-0-1  
Source VLANs :  
Receive Only :  
Transmit Only :  
Both :  
Destination Port : eth-0-2 eth-0-3
```

5

Configuring Remote Mirror

5.1 Configuring Remote Mirror

5.1.1 Overview

Remote mirror supports source ports, source VLANs, and destination ports on different switches (or different switch stacks), enabling remote monitoring of multiple switches across your network.

5.1.2 Terminology

The following describes concepts and terminology associated with remote mirror configuration.

Remote Mirror session

A remote mirror session is an association of some local source ports and vlans with a remote destination vlan, which has a specified out-going port.

The concepts of source ports and vlans in a remote mirror source session are as same as the local mirror.

A remote dest has these characteristics:

- It is a vlan with a specified out going port.
- The remote VLAN range should be 2 to 4094. If the VLAN isn't created in system, user can not configure this VLAN as mirror remote vlan.
- The out going port should be a physical port. User should manually check if the out going port can transfer mirrored packets.

- Monitor traffic packets are inserted a tag with the remote VLAN ID and directed over the specified out going port to the mirror destination session device.
- It is recommended to configure remote mirror's destination port as switch port. Users should add the destination port to the remote vlan otherwise the mirrored packet can not be transmitted out.

5.1.3 Topology

The below figure shows source ports on Switch A. The traffic for each remote mirror session is carried over a user-specified remote mirror VLAN that is dedicated for that remote mirror session in all participating switches. The remote mirror traffic from the source ports or VLANs is copied into the remote mirror VLAN and forwarded over trunk ports carrying the remote mirror VLAN to a destination session monitoring the remote mirror VLAN. Each remote mirror source switch must have either ports or VLANs as remote mirror sources. The destination is always a physical port, as same as the local mirror.

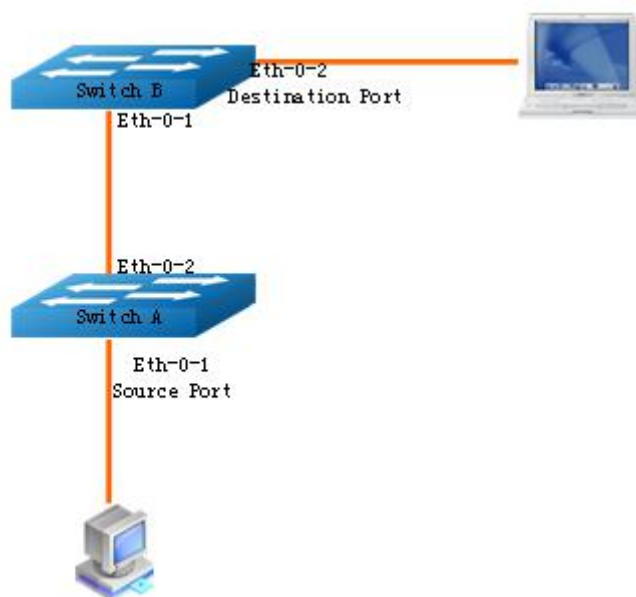


Figure 5-1 Remote Mirror

5.1.4 Configuration

Remote Mirror's configuration on Switch A

SwitchA# configure terminal	Enter the Configure mode
SwitchA(config)# vlan database	Enter the VLAN configure mode
SwitchA(config-vlan)# vlan 10	Create VLAN 10
SwitchA(config-vlan)# vlan 15	Create VLAN 15
SwitchA(config-vlan)# exit	Exit the Vlan database mode and enter the Configure mode
SwitchA(config)# interface eth-0-2	Enter the Interface mode
SwitchA(config-if)# no shutdown	Turn up the interface which is prepared to be the destination out-going port
SwitchA(config-if)# switchport mode trunk	Change the port mode as trunk
SwitchA(config-if)# switchport trunk allowed vlan add 15	Add eth-0-2 into vlan 15
SwitchA(config-if)# exit	Exit the Interface mode and enter the Configure mode
SwitchA(config)# interface eth-0-1	Enter the Interface mode
SwitchA(config-if)# switchport mode access	Change the port mode as access
SwitchA(config-if)# switchport access vlan 10	Add eth-0-1 into vlan 10
SwitchA(config)# monitor session 1 destination remote vlan 15 interface eth-0-2	Specify the mirror session and the remote destination vlan and out going port
SwitchA(config)# monitor session 1 source interface eth-0-1 both	Specify the mirror session and the source port (monitored port)
SwitchA(config)# end	Return to the EXEC mode
SwitchA # show monitor session 1	Display the session configuration

Remote Mirror's configuration on Switch B

1. Use “monitor session ID source vlan” command to get a copy of remote mirror packet on destination port. The packet is tagged.

SwitchB# configure terminal	Enter the Configure mode
SwitchB(config)# vlan database	Enter the VLAN configure mode
SwitchB(config-vlan)# vlan 15	Create VLAN 15
SwitchB(config-vlan)# exit	Exit the Vlan database mode and enter the Configure mode
SwitchB(config)# interface vlan15	Specify the interface (vlan15) to be configured and enter the Interface mode
SwitchB(config-if)# exit	Exit the Interface mode and enter the Configure mode
SwitchB(config)# interface eth-0-2	Enter the Interface mode
SwitchB(config-if)# no shutdown	Turn up the interface which is prepared to be the destination out-going port
SwitchB(config)# switch mode access	Change the port mode as access
SwitchA(config-if)# switchport access vlan 15	Add eth-0-2 into vlan 15
SwitchB(config)# interface eth-0-1	Enter the Interface mode
SwitchB(config-if)# no shutdown	Turn up the interface which is prepared to be the destination out-going port
SwitchB(config-if)# switchport mode trunk	Change the port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-1 into vlan 15
SwitchB(config-if)# exit	Exit the Interface mode and enter the Configure mode
SwitchB(config)# monitor session 1 destination interface eth-0-2	Specify the mirror session and the destination port
SwitchB(config)# monitor session 1 source vlan 15 rx	Specify the mirror session and the source vlan
SwitchB(config)# end	Return to the EXEC mode
SwitchB# show monitor session 1	Display the session configuration

2. Use access port to get the packet (you needn't any monitor session on switch B).

SwitchB# configure terminal	Enter the Configure mode
SwitchB(config)# no spanning-tree enable	Disable stp
SwitchB(config)# vlan database	Enter the VLAN configure mode
SwitchB(config-vlan)# vlan 15	Create VLAN 15
SwitchB(config-vlan)# exit	Exit the Vlan database mode and enter the Configure mode
SwitchB(config)# interface eth-0-2	Enter the Interface mode
SwitchB(config-if)# no shutdown	Turn up the interface which is prepared to be the destination out-going port
SwitchB(config-if)# switchport mode access	Change the port mode as access
SwitchB(config-if)# switchport access vlan 15	Add eth-0-2 into vlan 15
SwitchB(config)# interface eth-0-1	Enter the Interface mode
SwitchB(config-if)# no shutdown	Turn up the interface which is prepared to be the destination out-going port
SwitchB(config-if)# switchport mode trunk	Change the port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-1 into vlan 15
SwitchB(config-if)# exit	Exit the Interface mode and enter the Configure mode

3. Use trunk port to get tagged packet (you needn't any monitor session on switch B).

SwitchB# configure terminal	Enter the Configure mode
SwitchB(config)# no spanning-tree enable	Disable stp
SwitchB(config)# vlan database	Enter the VLAN configure mode
SwitchB(config-vlan)# vlan 15	Create VLAN 15
SwitchB(config-if)# exit	Exit the Vlan database mode and enter the Configure mode
SwitchB(config)# interface eth-0-2	Enter the Interface mode
SwitchB(config-if)# no shutdown	Turn up the interface which is preparint to be the destination out-going port

SwitchB(config-if)# switchport mode trunk	Change the port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-2 into vlan 15
SwitchB(config)# interface eth-0-1	Enter the Interface mode
SwitchB(config-if)# no shutdown	Turn up the interface which is preparint to be the destination out-going port
SwitchB(config-if)# switchport mode trunk	Change the port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-1 into vlan 15
SwitchB(config-if)# exit	Exit the Interface mode and enter the Configure mode



Use method 2 and method 3 might cause system leaning the Mac of mirrored packets and lead the FDB table exhausted.

5.1.5 Validation

This example shows how to set up a mirror session, session 1, for monitoring source port traffic to a destination port. You can use show monitor session to see the configuration.

SwitchA # show monitor session 1

```

Session 1
-----
Status          : Valid
Type            : Remote Session
Source Ports    :
  Receive Only  :
  Transmit Only :
  Both          : eth-0-1
Source VLANs    :
  Receive Only  :
  Transmit Only :
  Both          :
Destination Port : eth-0-2
Destination remote VLAN : 15

```

SwitchB # show monitor session 1

```
Session 1
-----
Status      : Valid
Type        : Local Session
Source Ports :
  Receive Only :
  Transmit Only :
  Both :
Source VLANs :
  Receive Only : 15
  Transmit Only :
  Both :
Destination Port : eth-0-2
```

5.2 Configuring Mac Escape for Remote Mirror

5.2.1 Overview

Mac escape is a sub-feature of remote mirror. It only affects the result of remote mirror.

A Mac escape entry includes a Mac address and a Mac Mask. When Mac escape entries are set, the packets whose MAC-DA match the entries should not be mirrored to the remote destination vlan. User can prevent protocol packed mirrored to remote by set some Mac escape entries.

5.2.2 Topology

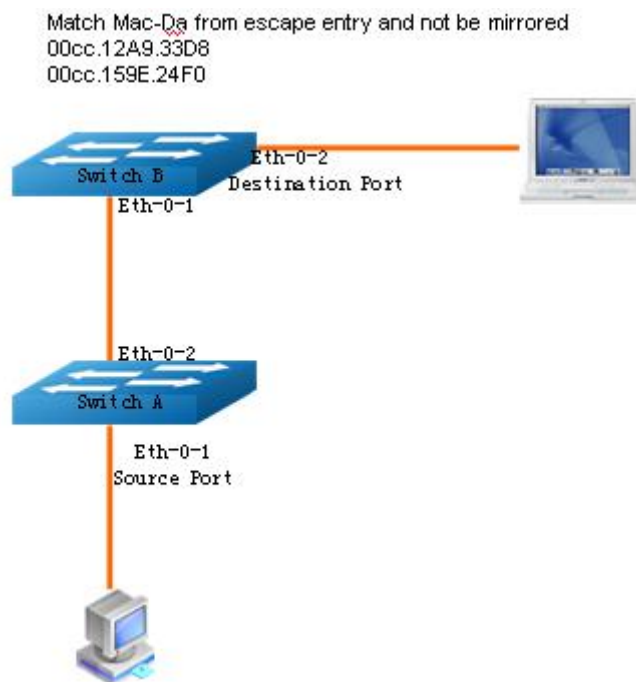


Figure 5-2 Mac Escape

5.2.3 Configuration

SwitchA #configure terminal	Enter the Configure mode.
SwitchA(config)# monitor mac escape 00cc.12A9.33D8 ffff.ffff.ffff	Create a Mac escape entry
SwitchA(config)# monitor mac escape 00cc.159E.24F0 ffff.ffff.ffff	Create another Mac escape entry
SwitchA(config)# end	Return to the EXEC mode
SwitchA# show monitor mac escape	Display the Mac escape configuration

5.2.4 Validation

This example shows how to set up the mac escape entries. You can use show monitor mac escape to see the configuration.

SwitchA # show monitor mac escape

```
-----  
monitor rspan mac escape database  
-----  
count      : 2  
-----  
Mac        : 00:cc:12:a9:33:d8  
Mask       : ff:ff:ff:ff:ff:ff  
Mac        : 00:cc:15:9e:24:f0  
Mask       : ff:ff:ff:ff:ff:ff  
-----
```

6

Configuring Device Management

6.1 Overview

User can manage the switch through the management port. The switch has two management ports: an Ethernet port and a console port.

6.2 Configuring console port for management

6.2.1 Configuration

The default console parameters of switch are:

- Baud rate default is 115200.
- Data bits default is 8.
- Stop bits default is 1.
- Parity settings default is none.

Before you can assign switch information, make sure you have connected a PC or terminal to the console port, and configured the PC or terminal software parameters to match the default console port parameters. After login in the switch, you can modify the console parameters.

Switch# configure terminal	Enter global configuration mode.
Switch(config)# line console 0	Enter line configuration mode, use line console 0 when you want to set console port access
Switch(config-line)# speed 19200	Set the console speed

6.2.2 Validation

After the above setting, console port parameter has been changed, and the PC or terminal can't configure the switch by console port. You must update PC or terminal console speed from 9600 to 19200 to match the new console parameter and can continue configure the switch by console port.

6.3 Configuring out band Ethernet port for management

In order to manage device by out band Ethernet port, you should configure management ip address first by console port.

6.3.1 Configuration

Switch# configure terminal	Enter the Configure mode.
Switch(config)# management ip address A.B.C.D/M	Configure switch management IPv4 address A.B.C.D - IP address of management port M - subnet mask
Switch(config)# management ipv6 address A:B::C/M	Configure switch management IPv6 address A:B::C – IPv6 address of management port M - subnet mask
Switch(config)# exit	Return to privileged EXEC mode
Switch#show management ip address	Verify the configured management IPv4 address
Switch#show management ipv6 address	Verify the configured management IPv6 address

6.3.2 Validation

After the above setting, you can use CLI 'show management ip address' or 'show management ipv6 address' to verify the configured management IP address. Also you can ping A.B.C.D from PC to verify the ip address.

Switch# show management ip address

```
Management IP address is: A.B.C.D/M
Gateway: 0.0.0.0
```

Switch # show management ipv6 address

```
Management IPv6 address is: 2001:1000::1/96
Gateway: ::
```

6.4 Configuring Temperature

The switch supports temperature alarm management. You can configure three temperature thresholds: low, high and critical. When switch temperature is lower than low threshold or higher than higher threshold, the switch will be alarm. If the switch temperature is higher than critical threshold, the switch will cut off its power automatically.

6.4.1 Configuring temperature threshold

Switch# configure terminal	Enter global configuration mode
Switch(config)# temperature 5 70 85	Setting new thresholds, unit is Celsius scale
Switch(config)# exit	Exit global configuration mode
Switch# show environment	Verify the configuration about threshold

6.4.2 Validation

Switch# show environment

```
-----
Sensor status (Degree Centigrade):
Index Temperature Lower_alarm Upper_alarm Critical_limit
1      49           5           70           85
```

6.5 Configuring Fan

The switch supports to manage fan automatically. If the fan is fail or the fan tray is absent, the switch will be alarm. And if the fan tray supports speed-adjust, the switch can adjust the fan speed depending on the real-time temperature. The switch has three temperature thresholds: Tlow=50, Thigh=65 and Tcrit=80 Celsius scales. If Temperature<Tlow, the fan will stall; if Tlow<=Temperature<Thigh, the fan will run on 30% speed rate; if Thigh<=Temperature<Tcrit, the fan will run on 70% speed rate; if Tcrit>=Temperature, the fan will run on 100% speed rate. And there has a temperature hysteresis Thyst=2 Celsius scales. Assuming temperature has previously crossed above Tlow, Thigh or Tcrit, then the temperature must drop below the points corresponding Thyst(Tlow-Thyst, Thigh-Thyst or Tcrit-Thyst) in order for the condition to drive fan speed rate to lower level. For example:

- temperature is 58 Celsius scales, the fan speed rate is 30%; (Tlow<58<Thigh)
- temperature increases to 65 Celsius scales, the fan speed rate is 70%;(Thigh=65)
- temperature decreases to 63 Celsius scales, the fan speed rate is still 70%;(Thigh-Thyst=63)
- temperature decreases to 62 Celsius scales, the fan speed rate is 30%;(62<Thigh-Thyst)

6.5.1 Configuration

The Tlow, Thigh, Tcrit, Thyst and fan speed rate for each temperature threshold are hard code, and couldn't be modified.

6.5.2 Validation

User can change the environment temperature to verify the fan auto management.

Switch# show environment

```
Fan tray status:
Index      Status
1          PRESENT
FanIndex   Status  SpeedRate  Mode
1-1        OK      80%        Auto
1-2        OK      80%        Auto
1-3        OK      80%        Auto
1-4        OK      80%        Auto
```



```
-----
Sensor status (Degree Centigrade):
Index Temperature Lower_alarm Upper_alarm Critical_limit
1      50           5           75           90
```

6.6 Configuring Power

The switch supports to manage power status automatically. If the power is failed or the fan in power is failed, the switch will be alarm. If power is removed or inserted, the switch will notice user also.

6.6.1 Configuration

This function has no configuration command.

6.6.2 Validation

User can show the power status to verify the power status.

Switch# show environment

```
-----
Power status:
Index      Status    Power    Type      Fans      Control
1          PRESENT   OK       AC        -         -
2          ABSENT    -        -         -         -
3          PRESENT   OK       DC (PoE) -         -
-----
```

6.7 Configuring Transceiver

The switch supports manage the transceiver information, and the transceiver information includes basic information and diagnostic information. The basic information includes transceiver type, vendor name, PN, S/N, wavelength and link length for supported type. The diagnostic information includes real-time temperature, voltage, current, optical transmit power, optical receive power and the threshold about these parameters. If the transceiver is inserted or removed, the real-time parameter is out of threshold, the switch will notice the users.

6.7.1 Configuration

This function has no configuration command.

6.7.2 Validation

User can show the transceiver information to verify this function.

Switch# show transceiver detail

```
Port eth-1-2 transceiver info:
Transceiver Type: 10G Base-SR
Transceiver Vendor Name : OEM
Transceiver PN          : SFP-10GB-SR
Transceiver S/N         : 201033PST1077C
Transceiver Output Wavelength: 850 nm
Supported Link Type and Length:
    Link Length for 50/125um multi-mode fiber: 80 m
    Link Length for 62.5/125um multi-mode fiber: 30 m
```

```
-----
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
The threshold values are calibrated.
```

```
-----
          High Alarm  High Warn  Low Warn  Low Alarm
Temperature Threshold  Threshold  Threshold  Threshold
Port  (Celsius)      (Celsius)  (Celsius)  (Celsius)  (Celsius)
-----
eth-1-2  25.92        95.00      90.00      -20.00      -25.00
```

```
-----
          High Alarm  High Warn  Low Warn  Low Alarm
Voltage   Threshold  Threshold  Threshold  Threshold
Port  (Volts)      (Volts)    (Volts)    (Volts)    (Volts)
-----
eth-1-2  3.32        3.80       3.70       2.90       2.80
```

```
-----
          High Alarm  High Warn  Low Warn  Low Alarm
Current   Threshold  Threshold  Threshold  Threshold
Port  (milliamperes)  (mA)       (mA)       (mA)       (mA)
-----
eth-1-2  6.41        20.00      18.00      1.00       0.50
```

```
-----
          High Alarm  High Warn  Low Warn  Low Alarm
Transmit Power Threshold  Threshold  Threshold  Threshold
Port  (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-----
eth-1-2  -2.41      2.01       1.00      -6.99      -7.96
```


	Optical	High Alarm	High Warn	Low Warn	Low Alarm
	Receive Power	Threshold	Threshold	Threshold	Threshold
Port	(dBm)	(dBm)	(dBm)	(dBm)	(dBm)

eth-1-2	-12	-	1.00	0.00	-19.00 -20.00

6.8 Upgrade bootrom

The switch supports to upgrade the bootrom image when system is running. And after upgrading, you must reboot the switch to take effect.

6.8.1 Configurations

Switch# copy mgmt-if tftp://10.10.29.160/bootrom.bin flash:/boot/	Copy bootloader image file from tftp server.
Switch# configure terminal	Enter global configuration mode.
Switch(config)# update bootrom flash:/boot/ bootrom.bin	Update bootrom from assigned file
Switch#(config)# exit	Exit global configuration mode
Switch# reboot	Restart device to confirm

6.8.2 Validation

After the above setting, you can show uboot version information of platform:

```
Switch# show version
...
EPLD Version is 1
BootRom Version is 3.0.2
```



When enable stacking, slave member don't support this command.

6.9 Upgrade EPLD

The switch supports to upgrade the EPLD image when system is running. And after upgrading, you must reboot the switch to take effect.

6.9.1 Configurations

Switch# copy mgmt-if tftp://10.10.29.160/vme_v1.0 flash:/boot/ vme_v1.0	Copy EPLD image file from tftp server
Switch# configure terminal	Enter global configuration mode
Switch(config)# update epld flash:/boot/vme_v1.0	Update epld from assigned file
Switch(config)# exit	Exit global configuration mode
Switch# reboot	Restart device to confirm

6.9.2 Validation

After the above setting, then power off and restart the device, you can show epld version information with command:

Switch# show version

```
.....  
EPLD Version is 1  
BootRom Version is 3.0.2  
System serial number is E045GD111005
```



When enable stacking, slave member don't support this command.

7

Configuring Bootrom

7.1 Overview

The main function of Bootrom is to initialize the board simply and load the system image to boot. You can use some necessary commands in bootrom mode.

Bootrom can load the system image both from TFTP server and persistent storage like flash. Then you can configure the Switch and TFTP server IP address as environment variables in Bootrom mode for boot the system image.

7.2 Configuring Boot from TFTP Server

7.2.1 Configurations

bootrom:> setenv bootcmd boot_tftp OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from TFTP server
bootrom:> saveenv	Save the configuration to persistent storage
bootrom:> reset	perform RESET of the CPU

bootrom:> setenv bootcmd boot_tftp_nopass OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from TFTP server with default configuration
bootrom:> saveenv	Save the configuration to persistent storage
bootrom:> reset	perform RESET of the CPU

bootrom:> boot_tftp OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from TFTP server immediately
bootrom:> boot_tftp_nopass OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from TFTP server with default configuration immediately

7.2.2 Validation

After the above setting, you can get show information

bootrom:> reset

```

.....
TFTP from server 10.10.29.160; our IP address is 10.10.29.118
Filename 'OS-ms-v3.1.9.it.r.bin'.
Load address: 0xaa00000
Loading: octeth0: Up 100 Mbps Full duplex (port 0)
#####
#####
done
Bytes transferred = 12314539 (bbe7ab hex), 1829 Kbytes/sec

```

7.3 Configuring Boot from Flash

7.3.1 Configurations

Step 1 Boot the system through image OS-ms-v3.1.9.it.r.bin from flash, details information as follows.

bootrom:> setenv bootcmd boot_flash OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from flash
bootrom:> saveenv	Save the configuration to persistent storage
bootrom:> reset	perform RESET of the CPU

Step 2 Boot the system through image OS-ms-v3.1.9.it.r.bin from flash with default configuration, details information as follows.

bootrom:> setenv bootcmd boot_flash_nopass OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from flash with default configuration
bootrom:> saveenv	Save the configuration to persistent storage
bootrom:> reset	perform RESET of the CPU
Do you want to revert to the default config file ? [Y N E]:Y	Y:revert to the default config file N:just revert the login configuration to the default E: exit this command

Step 3 Boot the system through image OS-ms-v3.1.9.it.r.bin from flash immediately, details information as follows.

bootrom:> boot_flash OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from flash immediately
--	--

Step 4 Boot the system through image OS-ms-v3.1.9.it.r.bin from flash with default configuration immediately, details information as follows.

bootrom:> boot_flash_nopass OS-ms-v3.1.9.it.r.bin	Boot the system through image OS-ms-v3.1.9.it.r.bin from flash with default configuration immediately
Do you want to revert to the default config file ? [Y N E]:Y	Y:revert to the default config file N:just revert the login configuration to the default E: exit this command

7.3.2 Validation

After the above setting, you can get show information:

```
bootrom:> reset
```

```
.....
Do you want to revert to the default config file ? [Y|N|E]:Y
### JFFS2 loading '/boot/OS-ms-v3.1.9.it.r.bin' to 0xaa00000
Scanning JFFS2 FS: . done.
### JFFS2 load complete: 12314539 bytes loaded to 0xaa00000
## Booting image at 0aa00000 ...
Verifying Checksum ... OK
Uncompressing Kernel Image ... OK
.....
```

7.4 Set boot IP

7.4.1 Configurations

Step 1 Set Switch IP address , details information as follows.

bootrom:> setenv ipaddr 10.10.29.101	Set Switch IP address
bootrom:> saveenv	Save the configuration to persistent storage

Step 2 Set TFTP server IP address , details information as follows.

bootrom:> setenv ipserver 10.10.29.160	Set TFTP server IP address
bootrom:> saveenv	Save the configuration to persistent storage

7.4.2 Validation

After the above setting, you can get show information:

```
bootrom:> printenv
```

```
printenv
bootdelay=5
baudrate=9600
download_baudrate=9600
.....
stderr=serial
ipaddr=10.10.29.101
ipserver=10.10.29.160
```


Environment size: 856/2044 bytes

7.5 Upgrade bootrom

7.5.1 Configurations

bootrom:> upgrade_uboot bootrom.bin	upgrade the Bootrom image from TFTP server
-------------------------------------	--

7.5.2 Validation

After the above setting, you can get show information:

bootrom:> version

version

Bootrom 3.0.3 (Development build) (Build time: Aug 4 2011 - 11:47:06)

7.6 Set gateway IP

7.6.1 Configurations

Step 1 Set Switch gateway IP address , details information as follows.

bootrom:> setenv gatewayip 10.10.37.1	Set Switch gate way IP address
bootrom:> saveenv	Save the configuration to persistent storage

Step 2 Set network mask , details information as follows.

bootrom:> setenv netmask 255.255.255.0	Set network mask
bootrom:> saveenv	Save the configuration to persistent storage

7.6.2 Validation

After the above setting, you can get show information:

```
bootrom:> printenv
```

```
printenv
bootdelay=5
baudrate=9600
download_baudrate=9600
.....
stderr=serial
gatewayip=10.10.38.1
netmask=255.255.255.0

Environment size: 856/2044 bytes
```

8 Configuring Bootup Diagnostic

8.1 Overview

Bootup diagnostic is used to help user diagnose whether the hardware component of Switch is working normally, after the Switch is already bootup. The diagnostic item including EPLD, EEPROM, PHY, MAC and so on.

8.2 Configuration

The configuration of bootup diagnostic is as follow.

Switch# configure terminal	Enter the Configure mode
Switch(config)# diagnostic bootup level minimal	Set the bootup diagnostic level to minimal
Switch(config)# exit	Exit the global configuration
Switch# show diagnostic bootup level	Show the bootup diagnostic level
Switch# reboot	Reboot the Switch

8.3 Validation

This example shows how to show the bootup diagnostic result.

Switch# show diagnostic bootup result detail

```
#####
Item Name      Attribute Result Time(usec)
1  EPLD TEST    C      Pass    57
2  EEPROM0 TEST C      Pass   101262
3  PHY TEST     C      Pass    1161
```

4	FAN TEST	C	Pass	4668
5	SENSOR TEST	C	Pass	5472
6	PSU TEST	C	Pass	1370
7	L2 UCAST FUNC TEST	C	Pass	40126

9

Configuring PoE

9.1 Overview

The main function of PoE is to pass electrical power safely, along with data, over Ethernet cabling. The standard is IEEE 802.3at and IEEE 302.3af.

System can support PSE external supplied power to plug or remove suddenly, and can detect the PSE supplied power status in 6s, then initiate the system PoE function. But we strongly don't recommend plugging or removing the PSE supplied power suddenly, as initiating the system PoE function will make the system busy then impact the performance of the total system.

If the PoE daughter card is absent, user configuration by CLI will be fail ignoring the status of PoE power status.

If the PoE card is present, the real behavior of user configuration is based on the PSE supplied power status. If the PSE supplied power is OK, the configuration will take effect and be stored in memory. If the PoE power status is off, the configuration will only be stored in memory.

When PoE card is present, if PSE supplied power status change from absence to OK, PoE will load PoE configuration from memory and PoE can work normally, if PSE supplied power status change from OK to absence, PoE will save the PoE configuration and PoE can't work.

When the current PSE voltage is lower than the 44 voltage or higher than the 57voltage, system should tell user by information. We strongly recommend that PSE supplied voltage is over 53V.

When the system total consumption is higher or lower than the alarm threshold of PSE budget at the first time, system will alarm user by information.

Whenever the PD status changed such as powered on, powered off , power error and so on, system will tell user by information.

When the PD is abnormal or PSE can't power on the 30 WPD, PSE may repeatedly process the IEEE standard power up flow. If PD status changes over 25 times in 60s, system will disable the port to protect PSE and PD, then alarm user by information.

System PSE max budget is up to 739.2W which support 24 ports up to 30W or 48 ports up to 15.4W or mixed situation.

When both PSE and PD have the same PI mode, the PSE can power up PD successfully. PSE only support alternative A mode which is that pin 1 and pin 2 is form one side of DC, pin 3 and pin 6 form other side.

Each port can supply DC power and support the length of 100 meters at most, Category 5(and Cat5e) cabling.

9.2 Terminology

Following is a brief description of terms and concepts used to describe PoE:

PoE: Power over Ethernet

PSE: Power-sourcing Equipment

PD: Powered Device

PI: Power Interface

9.3 Topology

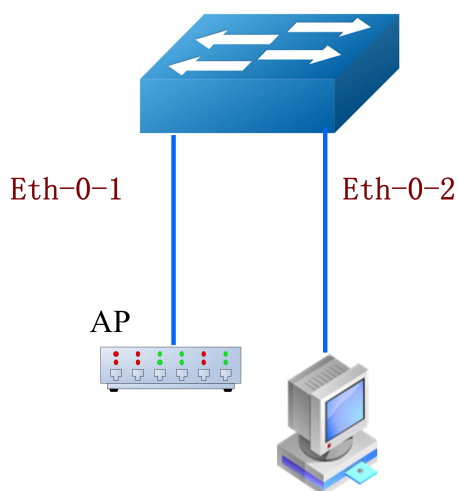


Figure 9-1 PoE Topology

9.4 Configuration

Configuring PSEdetails

Switch# configure terminal	Enter configuration mode
Switch(config)# poe max-budget 200000	Set max consumption limit of 200W
Switch(config)# poe power-management auto	Set power management mode to auto
Switch(config)# poe legacy enable	Enable legacy PD detection ability
Switch(config)# poe power-reserved 30	Set security reserved budget 30%
Switch(config)# poe power-threshold 80	Set consumption alarm threshold 80%



Set PSE power-management and legacy will trigger all the PDs powers off to make the PSE setting works.

The difference of two power-management mode is that port priority only takes effect in manual power-management mode.

The legacy PDs are devices that are not standard legacy device and some CISCO PD device.

The power-reserved percentage based on PSE budget is to prevent PD powered off from that consumption added suddenly leads to PSE overload and detect the consumption of new connected PD to decide whether the new connected PD will be powered on in system PoE management rule (e.g.: priority rule).

Configuring PoE port details

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# poe admin disable	Disable port Power over Ethernet
Switch(config-if)# poe budget 20000	Set port max consumption 20 Watt
Switch(config-if)# poe priority low	Set port priority to low
Switch(config-if)# poe admin disable time-range poeTimeRange	Set PoE time range of power off



There may be dangerous situation if PD isn't connected when port administration is force power mode.

If the port operating status is "protection off", you can disable and then enable the port to make port be normal. If the port operating status is "priority off" or "overload off", only the PoE system management automatically can make port be normal and PoE command can't work well

If the frequency of port status changing times is too high, PSE will disable the PD to protect PD and PSE from unknown dangerous situation.

The PD that exceeds its power budget will be disconnected due to overload and be punished in 60s time. The PSE will try to power on the overload PD after punish time. If the PD is still overload, PD will be disconnected and the previous punish time will be add 60s. If the PD works normal, the previous punish time will be subtracted 60s. The punish time can ascend step by step till 1 hour, if the PD is always overload when port punish time is over. The punish time can descend step by step till 0, when the PD is always normal but also port punish time is exist

In manual PM mode, system supports three port priorities: critical, high and low. A critical port is the highest priority; high priority is higher than low priority. The higher priority port which consumption suddenly increased but within the port max budget can snatch system budget from other port, when PSE is over available budget but within guard reserved budget. The lower priority port may be powered off, if system is overload.

If several ports belong to the same priority, the lower panel number port has the higher priority.

In auto PM mode, the priority rule is the same to manual PM mode, but port priority doesn't take effect and the lower panel number port has the higher priority.

Whether the new connected PD will be powered on is based on port priority rule and PSE reserved budget.

Time-range supports two modes: periodic and absolute, please refer to time-range command.

If system matches the start time of time-range interval, PSE will power off the PD, If system is over the end time of time-range interval, PSE will restore the previous poe admin ability.

9.5 Validation

The result of show running-config is as follows.

Switch# show running-config

```
poe max-budget 200000
poe legacy enable
poe power-management auto
poe power-reserved 30
poe power-threshold 80
!
vlan database
!

time-range poeTimeRange
  absolute start 12:12:12 Jun 13 2012 end 20:12:12 Jun 13 2012
!
interface eth-0-1
  poe admin disable
  poe budget 20000
  poe admin disable time-range poeTimeRange
!
```

Switch# show poe interface brief

Interface	Admin	Priority	Operating	Class	CurPower	MaxPower
				IEEE	Watts	Watts
-----	-----	-----	-----	----	-----	-----
eth-0-1	disable	low	off	-	0.00	20.00
eth-0-2	enabled	critical	detection	-	0.00	30.00
eth-0-3	enabled	critical	detection	-	0.00	30.00
eth-0-4	enabled	critical	detection	-	0.00	30.00

Switch# show poe interface power eth-0-1

Interface	CurPower	AverPower	PeakPower	MaxPower
	Watts	Watts	Watts	Watts
-----	-----	-----	-----	-----
eth-0-1	0.00	0.00	0.00	20.00

10

Configuring SmartConfig

10.1 Overview

SmartConfig is a smart method of switch initial configuration. After enabling SmartConfig, switch will start to download configuration file or image file from tftp server , if not finding startup-config file at startup. Then switch will install these file , and it will reboot itself if had downloaded image file.

Note that we use deploy file to control the configuration file and image file downloaded by switch. Switch fetch these file according the deploy file, which is a XML-formated file. The deploy file named smartdeploy.xml , while its content like below:

```
<SmartDeploy>

  <ftype>init</ftype>

  <hostprefix>Bruce</hostprefix>

  <defItem>

    <option>enable</option>

    <image>def.bin</image>

    <config>def.cfg</config>

  </defItem>

  <groups>
```

```
<Item>

  <type>MAC</type>

  <value>001e.0808.9100</value>

  <image>FSOS.bin</image>

  <config>startup.cfg</config>

</Item>

<Item>

  <type>productid</type>

  <value>09SWITCH-E48-10</value>

  <image>productid.bin</image>

  <config>productid.cfg</config>

</Item>

<Item>

  <type>SN</type>

  <value>E054GD116004</value>

  <image>sn.bin</image>

  <config>sn.cfg</config>

</Item>

</groups>

</SmartDeploy>
```

There are three kind of item used by switch to find out image file and configuration file fit itself. Switch will search fit item according sequence like MAC, SN , productid。 We just specify the file name in the deploy file, and place all these file on tftp server.

10.2 Topology

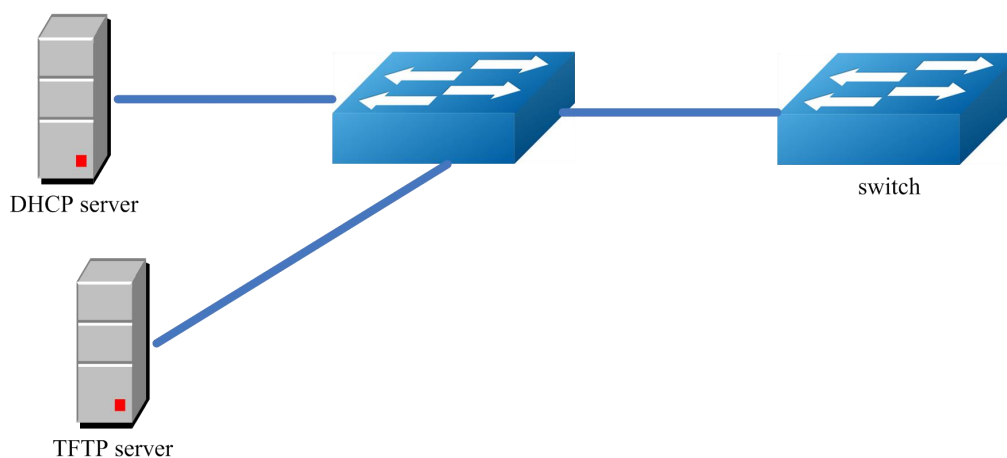


Figure 10-1 SmartConfig Topology

This figure is the network topology of testing SmartConfig function. We need two switches and two linux boxes to construct the test bed. "switch" in the figure is the switch we enable SmartConfig on. Note that the address of TFTP server provided by DHCP server can be used by switch to connect to TFTP server directly or via routes.

10.3 Configuration

Configuring Smartconfig

Switch#configure terminal	Enter the Configure mode
Switch(config)#smart-config initial-switch-deployment	Enable SmartConfig
Switch (config)#exit	Exit the Configure mode

SmartConfig was enable default, so we just make sure there is no startup-config.conf file. Then switch will start SmartConfig next boot. And we can delete startup-config.conf manually, so that Smartconfig will work after reboot.

Procedure of configure SmartConfig as fallow:

1 Configure smartdeploy.xml file, and place it with image file, configuration file to tftp server.

The directory must be like this :

```
/--  
  
|--smartconfig/  
    |--conf/  
    |--images/  
    |--smartdeploy.xml
```

Configuration files should be in conf directory and images should be in images directory.

2 Configure DHCP server, tftp server address option must be set;

3 Make sure there is no startup-config.conf file;

10.4 4 boot or reboot.Validation

Check SmartConfig configuration

Switch# show smart-config config

```
Smart-Config config:  
initial-switch-deployment: on  
hostname-prefix: on  
  
Send log message to console: on
```

11

Configuring Stacking

11.1 Overview

A switch stacking is a set of up to twenty-nine FS switches connected through their ports. One of the switches controls the operation of the stacking and is called the stack master. The stack master and the other switches in the stacking are stack members. The stack members use the FS stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

11.2 Topology

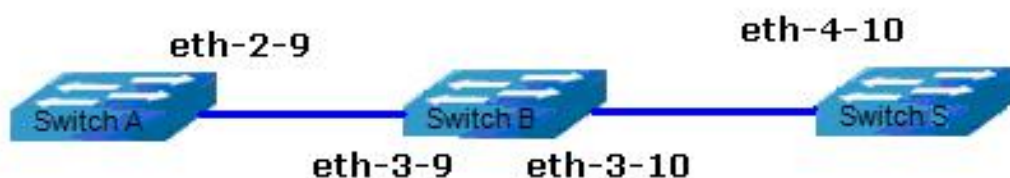


Figure 11-1 Stacking Topology

This figure is the network topology of testing Stacking function. We need three switches and to construct the test bed. "Switch" in the figure is the switch we enable stacking on.

11.3 Configuration

Configuring Stacking

Switch A, acted as a master stacking device:

SwitchA#configure terminal	Enter the Configure mode
SwitchA(config)#stack enable	Enable stacking
SwitchA(config)# stack master 2	Configure stacking master member ID
SwitchA(config)#stack member 2	Configure local device stack member ID
SwitchA(config)# interface eth-0-9	Enter the interface mode
SwitchA(config-if)#stack-trunk 1	Configure stacking port
SwitchA(config-if)#end	Configure EXEC mode
SwitchA#write	Save configure to startup-config file
SwitchA#reboot	Reboot Switch A
SwitchA# configure terminal	Enter the Configure mode, after switch A finish reloading.
SwitchA(config)# stack-switch 3 type 48t4x	Configure slave stacking device, member ID 3
SwitchA(config)# stack-switch 4 type 48t4x	Configure slave stacking device, member ID 4
SwitchA(config)# stack-switch 3 transmit stack-trunk 1	Configure the stacking port of slave stacking device
SwitchA(config)# stack-switch 4 transmit stack-trunk 1	Configure the stacking port of slave stacking device

Switch B, acted as a slave stacking device:

SwitchB#configure terminal	Enter the Configure mode
SwitchB(config)#stack enable	Enable stacking
SwitchB(config)# stack master 2	Configure stacking master member ID
SwitchB(config)#stack member 3	Configure local device stack member ID
SwitchB(config)# stack-switch 2 transmit stack-trunk 1	Configure the stacking port of master stacking device
SwitchB(config)# stack-switch 4 transmit stack-trunk 2	Configure the stacking port of slave stacking device
SwitchB(config)# interface eth-0-9	Enter the interface mode
SwitchB(config-if)#stack-trunk 1	Configure stacking port
SwitchB(config)# interface eth-0-10	Enter the interface mode

SwitchB(config-if)#stack-trunk 2	Configure stacking port
SwitchB(config-if)#end	Configure EXEC mode
SwitchB#write	Save configure to startup-config file
SwitchB#reboot	Reboot Switch B

Switch S, acted as a slave stacking device:

SwitchS#configure terminal	Enter the Configure mode
SwitchS(config)#stack enable	Enable stacking
SwitchS(config)# stack master 2	Configure stacking master member ID
SwitchS(config)#stack member 4	Configure local device stack member ID
SwitchS(config)# stack-switch 2 transmit stack-trunk 1	Configure the stacking port of master stacking device
SwitchS(config)# stack-switch 3 transmit stack-trunk 1	Configure the stacking port of slave stacking device
SwitchS(config)# interface eth-0-10	Enter the interface mode
SwitchS(config-if)#stack-trunk 1	Configure stacking port
SwitchS(config-if)#end	Configure EXEC mode
SwitchS#write	Save configure to startup-config file
SwitchS#reboot	Reboot Switch S

11.4 Validation

Check stacking device status

SwitchA# show stack-switch

Mem	Role	Config	Current	Port	SwVersion	SerialNo
=====						
*2	Master	E350_48T4XG2Q	ready	52	5.0.0.10.it	
3	Slave	E350_48T4XG2Q	ready	52	5.0.0.10.it	
4	Slave	E350_48T4XG2Q	absent	52		

11.5 Warning

Stacking port(eth-2-9,eth-3-9....), should be configured stack-trunk only, without others configuration.

SwitchA# show running-config interface eth-2-9

```
Building configuration...
!
interface eth-2-9
  stack-trunk 1
!
```

Stacking device's software version should be same, otherwise, the slave device will be reload.

11.6 Remove Stacking

Switch A, acted as a master stacking device. User can configure “no stack enable” , if the device don't be wanted to as a stacking device.

SwitchA#configure terminal	Enter the Configure mode
SwitchA(config)#no stack enable	Remove stacking
SwitchA(config-if)#end	Configure EXEC mode
SwitchA#write	Save configure to startup-config file
SwitchA#reboot	Reboot Switch A

12 Reboot Logs

12.1 Overview

FS switch support display reboot logs. Depend on these logs, user can judge the reboot reasons of a switch. The reboot reasons include Manual Reboot, Power Off or Other Reasons. Also, user can clear the reboot logs through a command.

12.2 Validation

The following example shows how to display reboot logs :

Switch# show reboot-info

Times	Reboot Type	Reboot Time (DST)
1	MANUAL	2000/01/01 01:21:35
2	MANUAL	2000/01/01 02:07:52
3	MANUAL	2000/01/01 02:24:59
4	MANUAL	2000/01/01 03:28:58
5	MANUAL	2000/01/01 03:43:02
6	MANUAL	2000/01/01 03:49:51
7	MANUAL	2000/01/01 04:01:23
8	MANUAL	2000/01/01 04:42:40
9	MANUAL	2000/01/01 04:49:27
10	MANUAL	2000/01/01 20:59:20

The following example shows how to clear reboot logs :

Switch(config)# reset reboot-info

12.3 Warning

User can find no more than ten reboot logs through this command, to find more reboot logs, can refer to the following file: `flash:/reboot-info/reboot_info.log`