Content

Chapter 1 Port Configuration

1.1 Introduction to Port

Switch contains 48 10G optical ports and 4 4x10G optical ports, each 4x10G optical port can be distributed into 4 10G optical ports and they support the same configuration and property with the ordinary SFP+ physical ports. After the 4x10G port distributed, a special one-to-four cable can be used to connect them.

If the user needs to configure some network ports, he/she can use the interface ethernet <interface-list> command to enter the appropriate Ethernet port configuration mode, where <interface-list> stands for one or more ports. If <interface-list> contains multiple ports, special characters such as ';' or '-' can be used to separate ports, ';' is used for discrete port numbers and '-' is used for consecutive port numbers. Suppose an operation should be performed on ports 2,3,4,5 the command would look like: interface ethernet 1/0/2-5. Port speed, duplex mode and traffic control can be configured under Ethernet Port Mode causing the performance of the corresponding network ports to change accordingly.

1.2 Network Port Configuration Task List

1. Enter the network port configuration mode
2. Configure the properties for the network ports
   (1) Enable/Disable ports
   (2) Configure port names
   (3) Configure port speed and duplex mode
   (4) Configure bandwidth control
   (5) Configure traffic control
   (6) Enable/Disable port loopback function
   (7) Configure broadcast storm control function for the switch
   (8) Configure scan port mode
   (9) Configure rate-violation control of the port
   (10) Configure interval of port-rate-statistics

1. Enter the Ethernet port configuration mode

Command	Explanation
Global Mode	
interface ethernet <*interface-list*>	Enters the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	Explanation
Port Mode	
shutdown **no shutdown**	Enables/Disables specified ports.
description <string> **no description**	Specifies or cancels the name of specified ports.
speed-duplex {auto [10 [100 [1000]] [auto | full | half |]] | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected | no-phy-integrated | phy-integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}| force10g-full} **no speed-duplex**	Sets port speed and duplex mode of 100/1000Base-TX or 100Base-FX ports. The no format of this command restores the default setting, i.e., negotiates speed and duplex mode automatically.
bandwidth control *<bandwidth>* [both | receive | transmit] **no bandwidth control**	Sets or cancels the bandwidth used for incoming/outgoing traffic for specified ports.
flow control **no flow control**	Enables/Disables traffic control function for specified ports.
loopback **no loopback**	Enables/Disables loopback test function for specified ports.
storm-control {unicast | broadcast | multicast} <packets>	Enables the storm control function for broadcasts, multicasts and unicasts with unknown destinations (short for broadcast), and sets the allowed broadcast packet number; the no format of this command disables the broadcast storm control function.
port-scan-mode {interrupt | poll} **no port-scan-mode**	Configure port-scan-mode as interrupt or poll mode, the no command restores the default port-scan-mode.
rate-violation <200-2000000> [recovery <0-86400>] **no rate-violation**	Set the max packet reception rate of a port. If the rate of the received packet violates the packet reception rate, shut down this port and configure the recovery time, the default is 300s. The no command will disable the rate-violation function of a port.

Global Mode	
port-rate-statistics interval <interval -value>	Configure the interval of port-rate-statistics.

1.3 Port Configuration Example

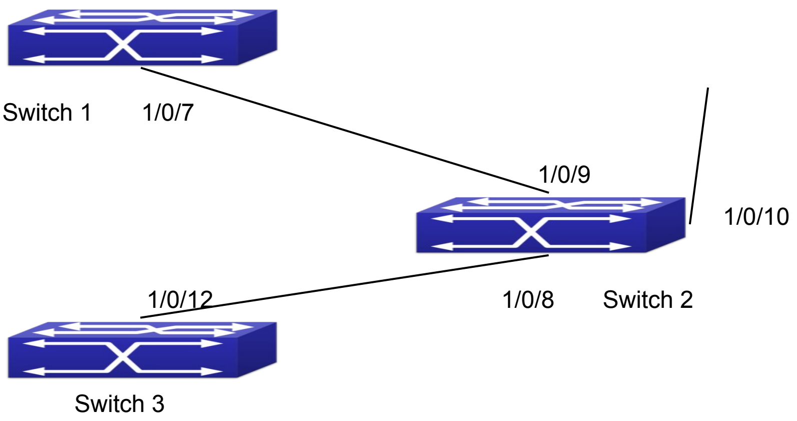

Fig 1-1 Port Configuration Example

No VLAN has been configured in the switches, default VLAN1 is used.

Switch	**Port**	**Property**
Switch1	1/0/7	Ingress bandwidth limit: 50 M
Switch2	1/0/8	Mirror source port
	1/0/9	1000Mbps full, mirror source port
	1/0/10	10000Mbps full, mirror destination port
Switch3	1/0/12	1000Mbps full

The configurations are listed below:

Switch1:

```
Switch1(config)#interface ethernet 1/0/7
Switch1(Config-If-Ethernet1/0/7)#bandwidth control 50 both
```

Switch2:

```
Switch2(config)#interface ethernet 1/0/9
Switch2(Config-If-Ethernet1/0/9)#speed-duplex forceg-full
Switch2(Config-If-Ethernet1/0/9)#exit
Switch2(config)#interface ethernet 1/0/10
Switch2(Config-If-Ethernet1/0/10)#speed-duplex force10g-full
Switch2(Config-If-Ethernet1/0/10)#exit
Switch2(config)#monitor session 1 source interface ethernet 1/0/8;1/0/9
Switch2(config)#monitor session 1 destination interface ethernet 1/0/10
```

Switch3:

```
Switch3(config)#interface ethernet 1/0/12
Switch3(Config-If-Ethernet1/0/12)#speed-duplex force1g-full
Switch3(Config-If-Ethernet1/0/12)#exit
```

1.4 Port Troubleshooting

Here are some situations that frequently occurs in port configuration and the advised solutions:

☞ Two connected fiber interfaces won’t link up if one interface is set to auto-negotiation but the other to forced speed/duplex. This is determined by IEEE 802.3.

☞ The following combinations are not recommended: enabling traffic control as well as setting multicast limiting for the same port; setting broadcast, multicast and unknown destination unicast control as well as port bandwidth limiting for the same port. If such combinations are set, the port throughput may fall below the expected performance.

Chapter 2 Port Isolation Function Configuration

2.1 Introduction to Port Isolation Function

Port isolation is an independent port-based function working in an inter-port way, which isolates flows of different ports from each other. With the help of port isolation, users can isolate ports within a VLAN to save VLAN resources and enhance network security. After this function is configured, the ports in a port isolation group will be isolated from each other, while ports belonging to different isolation groups or no such group can forward data to one another normally. No more than 16 port isolation groups can a switch have.

2.2 Task Sequence of Port Isolation

1. Create an isolate port group
2. Add Ethernet ports into the group
3. Specify the flow to be isolated
4. Display the configuration of port isolation

1. Create an isolate port group

Command	Explanation
Global Mode	
isolate-port group <*WORD*> **no isolate-port group <*WORD*>**	Set a port isolation group; the no operation of this command will delete the port isolation group.

2. Add Ethernet ports into the group

Command	Explanation
Global Mode	
isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*> **no isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*>**	Add one port or a group of ports into a port isolation group to isolate, which will become isolated from the other ports in the group; the no operation of this command will remove one port or a group of ports out of a port isolation group.

3. Specify the flow to be isolated

Command	Explanation
Global Mode	
isolate-port apply [<l2|l3|all>]	Apply the port isolation configuration to isolate layer-2 flows, layer-3 flows or all flows.

4. Display the configuration of port isolation

Command	Explanation
Admin Mode and global Mode	
show isolate-port group [*<WORD>*]	Display the configuration of port isolation, including all configured port isolation groups and Ethernet ports in each group.

2.3 Port Isolation Function Typical Examples

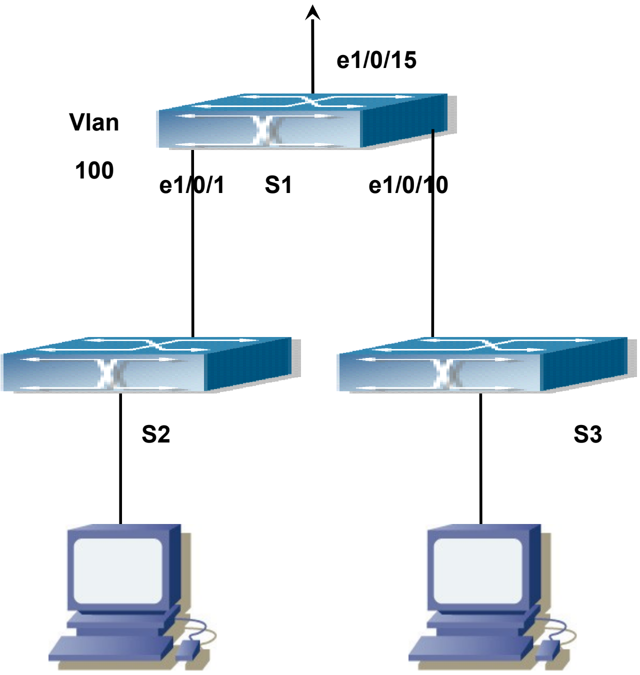

Fig 2-1 Typical example of port isolation function

The topology and configuration of switches are showed in the figure above, with e1/0/1, e1/0/10 and e1/0/15 all belonging to VLAN 100. The requirement is that, after port isolation is enabled on switch S1, e1/0/1 and e1/0/10 on switch S1 can not communicate with each other, while both of them can communicate with the uplink port e1/0/15. That is, the communication between any pair of downlink ports is disabled while that between any downlink port and a specified uplink port is normal. The uplink port can communicate with any port normally.

The configuration of S1:

```
Switch(config)#isolate-port group test
Switch(config)#isolate-port group test switchport interface ethernet 1/0/1;1/0/10
```

Chapter 3 Port Loopback Detection Function Configuration

3.1 Introduction to Port Loopback Detection Function

With the development of switches, more and more users begin to access the network through Ethernet switches. In enterprise network, users access the network through layer-2 switches, which means urgent demands for both internet and the internal layer 2 Interworking. When layer 2 Interworking is required, the messages will be forwarded through MAC addressing the accuracy of which is the key to a correct Interworking between users. In layer 2 switching, the messages are forwarded through MAC addressing. Layer 2 devices learn MAC addresses via learning source MAC address, that is, when the port receives a message from an unknown source MAC address, it will add this MAC to the receive port, so that the following messages with a destination of this MAC can be forwarded directly, which also means learn the MAC address once and for all to forward messages.

When a new source MAC is already learnt by the layer 2 device, only with a different source port, the original source port will be modified to the new one, which means to correspond the original MAC address with the new port. As a result, if there is any loopback existing in the link, all MAC addresses within the whole layer 2 network will be corresponded with the port where the loopback appears (usually the MAC address will be frequently shifted from one port to another), causing the layer 2 network collapsed. That is why it is a necessity to check port loopbacks in the network. When a loopback is detected, the detecting device should send alarms to the network management system, ensuring the network manager is able to discover, locate and solve the problem in the network and protect users from a long-lasting disconnected network.

Since detecting loopbacks can make dynamic judgment of the existence of loopbacks in the link and tell whether it has gone, the devices supporting port control (such as port isolation and port MAC address learning control) can maintain that automatically, which will not only reduce the burden of network managers but also response time, minimizing the effect caused loopbacks to the network.

3.2 Port Loopback Detection Function Configuration Task List

1．Configure the time interval of loopback detection
2．Enable the function of port loopback detection
3．Configure the control method of port loopback detection

4．Display and debug the relevant information of port loopback detection

5．Configure the loopback-detection control mode (automatic recovery enabled or not)

1．Configure the time interval of loopback detection

Command	Explanation
Global Mode	
loopback-detection interval-time <*loopback*> <*no-loopback*> **no loopback-detection interval-time**	Configure the time interval of loopback detection.

2．Enable the function of port loopback detection

Command	Explanation
Port Mode	
loopback-detection specified-vlan <vlan-*list*> **no loopback-detection specified-vlan <vlan-*list*>**	Enable and disable the function of port loopback detection.

3．Configure the control method of port loopback detection

Command	Explanation
Port Mode	
loopback-detection control {shutdown |block| learning} **no loopback-detection control**	Enable and disable the function of port loopback detection control.

4．Display and debug the relevant information of port loopback detection

Command	Explanation
Admin Mode	
debug loopback-detection **no debug loopback-detection**	Enable the debug information of the function module of port loopback detection. The no operation of this command will disable the debug information.
show loopback-detection [interface <*interface-list*>]	Display the state and result of the loopback detection of all ports, if no parameter is provided; otherwise, display the state and result of the corresponding ports.

5. Configure the loopback-detection control mode (automatic recovery enabled or

not)

Command	Explanation
Global Mode	
loopback-detection control-recovery timeout <0-3600>	Configure the loopback-detection control mode (automatic recovery enabled or not) or recovery time.

3.3 Port Loopback Detection Function Example

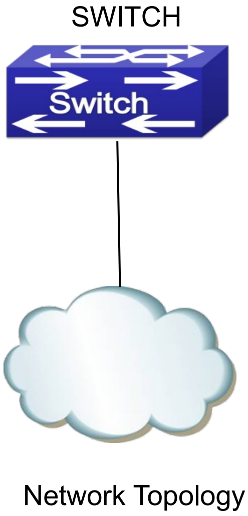

Fig 3-1 Typical example of port loopback detection

As shown in the above configuration, the switch will detect the existence of loopbacks in the network topology. After enabling the function of loopback detection on the port connecting the switch with the outside network, the switch will notify the connected network about the existence of a loopback, and control the port on the switch to guarantee the normal operation of the whole network.

The configuration task sequence of SWITCH:

```
Switch(config)#loopback-detection interval-time 35 15
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#loopback-detection special-vlan 1-3
Switch(Config-If-Ethernet1/0/1)#loopback-detection control block
```

If adopting the control method of block, MSTP should be globally enabled. And the corresponding relation between the spanning tree instance and the VLAN should be configured.

```
Switch(config)#spanning-tree
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#instance 2 vlan 2
Switch(Config-Mstp-Region)#
```

3.4 Port Loopback Detection Troubleshooting

The function of port loopback detection is disabled by default and should only be enabled if required.

Chapter 4 ULDP Function Configuration

4.1 Introduction to ULDP Function

Unidirectional link is a common error state of link in networks, especially in fiber links. Unidirectional link means that only one port of the link can receive messages from the other port, while the latter one can not receive messages from the former one. Since the physical layer of the link is connected and works normal, via the checking mechanism of the physical layer, communication problems between the devices can not be found. As shown in Graph, the problem in fiber connection can not be found through mechanisms in physical layer like automatic negotiation.

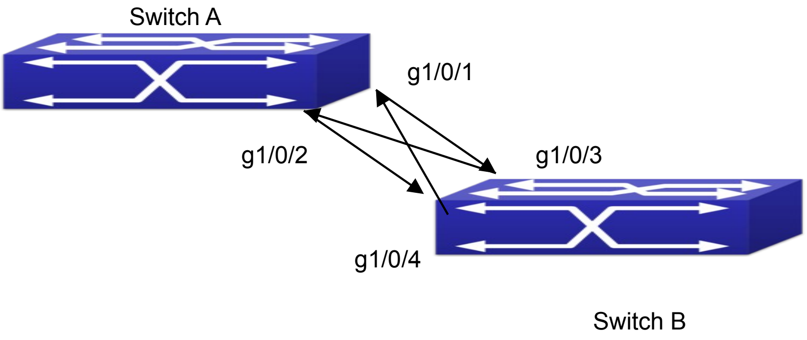

Fig 4-1 Fiber Cross Connection

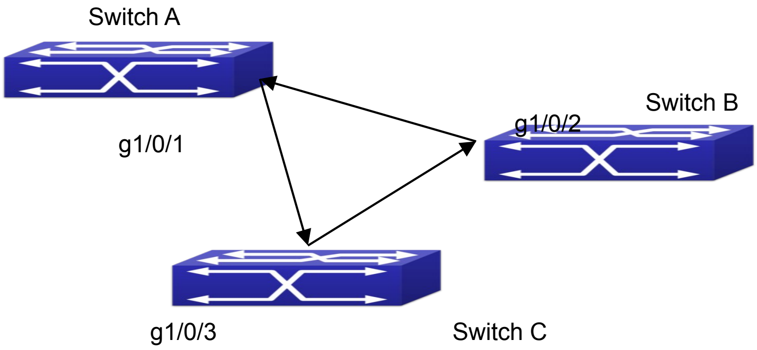

Fig 4-2 One End of Each Fiber Not Connected

This kind of problem often appears in the following situations: GBIC (Giga Bitrate Interface Converter) or interfaces have problems, software problems, hardware becomes unavailable or operates abnormally. Unidirectional link will cause a series of problems, such as spinning tree topological loop, broadcast black hole.

ULDP (Unidirectional Link Detection Protocol) can help avoid disasters that could happen in the situations mentioned above. In a switch connected via fibers or copper Ethernet line (like ultra five-kind twisted pair), ULDP can monitor the link state of physical links. Whenever a unidirectional link is discovered, it will send warnings to users and can disable the port automatically or manually according to users' configuration.

The ULDP of switches recognizes remote devices and check the correctness of link connections via interacting ULDP messages. When ULDP is enabled on a port, protocol state machine will be started, which means different types of messages will be sent at different states of the state machine to check the connection state of the link by exchanging information with remote devices. ULDP can dynamically study the interval at which the remote device sends notification messages and adjust the local TTL (time to live) according to that interval. Besides, ULDP provides the reset mechanism, when the port is disabled by ULDP, it can check again through reset mechanism. The time intervals of notification messages and reset in ULDP can be configured by users, so that ULDP can respond faster to connection errors in different network environments.

The premise of ULDP working normally is that link works in duplex mode, which means ULDP is enabled on both ends of the link, using the same method of authentication and password.

4.2 ULDP Configuration Task Sequence

1. Enable ULDP function globally
2. Enable ULDP function on a port
3. Configure aggressive mode globally
4. Configure aggressive mode on a port
5. Configure the method to shut down unidirectional link
6. Configure the interval of Hello messages
7. Configure the interval of Recovery
8. Reset the port shut down by ULDP
9. Display and debug the relative information of ULDP

1. Enable ULDP function globally

Command	Explanation
Global configuration mode	
uldp enable **uldp disable**	Globally enable or disable ULDP function.

2. Enable ULDP function on a port

Command	Explanation
Port configuration mode	
uldp enable **uldp disable**	Enable or disable ULDP function on a port.

3. Configure aggressive mode globally

Command	Explanation
Global configuration mode	
uldp aggressive-mode **no uldp aggressive-mode**	Set the global working mode.

4. Configure aggressive mode on a port

Command	Explanation
Port configuration mode	
uldp aggressive-mode **no uldp aggressive-mode**	Set the working mode of the port.

5. Configure the method to shut down unidirectional link

Command	Explanation
Global configuration mode	
uldp manual-shutdown **no uldp manual-shutdown**	Configure the method to shut down unidirectional link.

6. Configure the interval of Hello messages

Command	Explanation
Global configuration mode	
uldp hello-interval <*integer*> **no uldp hello-interval**	Configure the interval of Hello messages, ranging from 5 to 100 seconds. The value is 10 seconds by default.

7. Configure the interval of Recovery

Command	Explanation
Global configuration mode	
uldp recovery-time <*integer*> **no uldp recovery-time <*integer*>**	Configure the interval of Recovery reset, ranging from 30 to 86400 seconds. The value is 0 second by default.

8. Reset the port shut down by ULDP

Command	Explanation
Global configuration mode or port configuration mode	

uldp reset	Reset all ports in global configuration mode; Reset the specified port in port configuration mode.

9. Display and debug the relative information of ULDP

Command	Explanation
Admin mode	
show uldp [interface ethernet IFNAME]	Display ULDP information. No parameter means to display global ULDP information. The parameter specifying a port will display global information and the neighbor information of the port.
debug uldp fsm interface ethernet <*IFname*> **no debug uldp fsm interface ethernet <*IFname*>**	Enable or disable the debug switch of the state machine transition information on the specified port.
debug uldp error **no debug uldp error**	Enable or disable the debug switch of error information.
debug uldp event **no debug uldp event**	Enable or disable the debug switch of event information.
debug uldp packet {receive|send} **no debug uldp packet {receive|send}**	Enable or disable the type of messages can be received and sent on all ports.
debug uldp {hello|probe|echo| unidir| all} [receive|send] interface ethernet <*IFname*> **no debug uldp {hello|probe|echo| unidir|all} [receive|send] interface ethernet <*IFname*>**	Enable or disable the content detail of a particular type of messages can be received and sent on the specified port.

4.3 ULDP Function Typical Examples

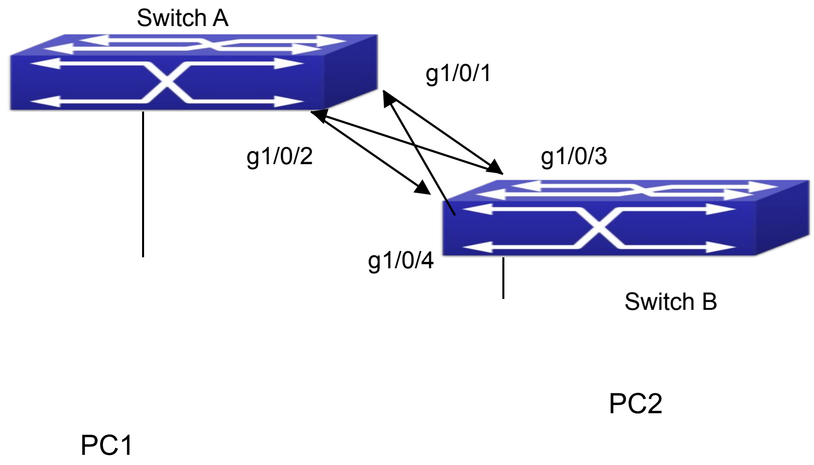

Fig 4-3 Fiber Cross Connection

In the network topology in Graph, port g1/0/1 and port g1/0/2 of SWITCH A as well as port g1/0/3 and port g1/0/4 of SWITCH B are all fiber ports. And the connection is cross connection. The physical layer is connected and works normally, but the data link layer is abnormal. ULDP can discover and disable this kind of error state of link. The final result is that port g1/0/1, g1/0/2 of SWITCH A and port g1/0/3, g1/0/4 of SWITCH B are all shut down by ULDP. Only when the connection is correct, can the ports work normally (won't be shut down).

Switch A configuration sequence:

```
SwitchA(config)#uldp enable
SwitchA(config)#interface ethernet 1/0/1
SwitchA(Config-If-Ethernet1/0/1)#uldp enable
SwitchA(Config-If-Ethernet1/0/1)#exit
SwitchA(config)#interface ethernet 1/0/2
SwitchA(Config-If-Ethernet1/0/2)#uldp enable
```

Switch B configuration sequence:

```
SwitchB(config)#uldp enable
SwitchB(config)#interface ethernet1/0/3
SwitchB(Config-If-Ethernet1/0/3)#uldp enable
SwitchB(Config-If-Ethernet1/0/3)#exit
SwitchB(config)#interface ethernet 1/0/4
SwitchB(Config-If-Ethernet1/0/4)#uldp enable
```

As a result, port g1/0/1, g1/0/2 of SWITCH A are all shut down by ULDP, and there is notification information on the CRT terminal of PC1.

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/1 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/1 shut down!

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/2 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/2 shutted down!

Port g1/0/3, and port g1/0/4 of SWITCH B are all shut down by ULDP, and there is notification information on the CRT terminal of PC2.

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/3 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/3 shutted down!

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/4 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/4 shutted down!

4.4 ULDP Troubleshooting

Configuration Notice:

☞ In order to ensure that ULDP can discover that the one of fiber ports has not connected or the ports are incorrectly cross connected, the ports have to work in duplex mode and have the same rate.

☞ If the automatic negotiation mechanism of the fiber ports with one port misconnected decides the working mode and rate of the ports, ULDP won’t take effect no matter enabled or not. In such situation, the port is considered as “Down”.

☞ In order to make sure that neighbors can be correctly created and unidirectional links can be correctly discovered, it is required that both end of the link should enable ULDP, using the same authentication method and password. At present, no password is needed on both ends.

☞ The hello interval of sending hello messages can be changed (it is10 seconds by default and ranges from 5 to 100 seconds) so that ULDP can respond faster to connection errors of links in different network environments. But this interval should be less than 1/3 of the STP convergence time. If the interval is too long, a STP loop will be generated before ULDP discovers and shuts down the unidirectional connection port. If the interval is too short, the network burden on the port will be increased, which means a reduced bandwidth.

☞ ULDP does not handle any LACP event. It treats every link of TRUNK group (like Port-channel, TRUNK ports) as independent, and handles each of them respectively.

☞ ULDP does not compact with similar protocols of other vendors, which means users can not use ULDP on one end and use other similar protocols on the other end.

☞ ULDP function is disabled by default. After globally enabling ULDP function, the debug switch can be enabled simultaneously to check the debug information. There are several DEBUG commands provided to print debug information, such as information of events, state machine, errors and messages. Different types of message information can also be printed according to different parameters.

☞ The Recovery timer is disabled by default and will only be enabled when the users have configured recovery time (30-86400 seconds).

☞ Reset command and reset mechanism can only reset the ports automatically shut down by ULDP. The ports shut down manually by users or by other modules won’t be reset by ULDP.

Chapter 5 LLDP Function Operation Configuration

5.1 Introduction to LLDP Function

Link Layer Discovery Protocol (LLDP) is a new protocol defined in 802.1ab. It enables neighbor devices to send notices of their own state to other devices, and enables all ports of every device to store information about them. If necessary, the ports can also send update information to the neighbor devices directly connected to them, and those neighbor devices will store the information in standard SNMP MIBs. The network management system can check the layer-two connection state from MIB. LLDP won't configure or control network elements or flows, but only report the configuration of layer-two. Another content of 802.1ab is to utilizing the information provided by LLDP to find the conflicts in layer-two. IEEE now uses the existing physical topology, interfaces and Entity MIBs of IETF.

To simplify, LLDP is a neighbor discovery protocol. It defines a standard method for Ethernet devices, such as switches, routers and WLAN access points, to enable them to notify their existence to other nodes in the network and store the discovery information of all neighbor devices. For example, the detail information of the device configuration and discovery can both use this protocol to advertise.

In specific, LLDP defines a general advertisement information set, a transportation advertisement protocol and a method to store the received advertisement information. The device to advertise its own information can put multiple pieces of advertisement information in one LAN data packet to transport. The type of transportation is the type length value (TLV) field. All devices supporting LLDP have to support device ID and port ID advertisement, but it is assumed that, most devices should also support system name, system description and system performance advertisement. System name and system description advertisement can also provide useful information for collecting network flow data. System description advertisement can include data such as the full name of the advertising device, hardware type of system, the version information of software operation system and so on.

802.1AB Link Layer Discovery Protocol will make searching the problems in an enterprise network an easier process and can strengthen the ability of network management tools to discover and maintain accurate network topology structure.

Many kinds of network management software use "Automated Discovery" function to trace the change and condition of topology, but most of them can reach layer-three and classify the devices into all IP subnets at best. This kind of data are very primitive, only referring to basic events like the adding and removing of relative devices instead of details about where and how these devices operate with the network.

Layer 2 discovery covers information like which devices have which ports, which switches connect to other devices and so on, it can also display the routs between clients, switches, routers, application servers and network servers. Such details will be very meaningful for schedule and investigate the source of network failure.

LLDP will be a very useful management tool, providing accurate information about network mirroring, flow data and searching network problems.

5.2 LLDP Function Configuration Task Sequence

1. Globally enable LLDP function
2. Configure the port-based LLDP function switch
3. Configure the operating state of port LLDP
4. Configure the intervals of LLDP updating messages
5. Configure the aging time multiplier of LLDP messages
6. Configure the sending delay of updating messages
7. Configure the intervals of sending Trap messages
8. Configure to enable the Trap function of the port
9. Configure the optional information-sending attribute of the port
10. Configure the size of space to store Remote Table of the port
11. Configure the type of operation when the Remote Table of the port is full
12. Display and debug the relative information of LLDP

1. Globally enable LLDP function

Command	Explanation
Global Mode	
lldp enable **lldp disable**	Globally enable or disable LLDP function.

2. Configure the port-base LLDP function switch

Command	Explanation
Port Mode	
lldp enable **lldp disable**	Configure the port-base LLDP function switch.

3. Configure the operating state of port LLDP

Command	Explanation
Port Mode	
lldp mode (send|receive|both|disable)	Configure the operating state of port LLDP.

4. Configure the intervals of LLDP updating messages

Command	Explanation
Global Mode	

lldp tx-interval <*integer*> **no lldp tx-interval**	Configure the intervals of LLDP updating messages as the specified value or default value.

5. Configure the aging time multiplier of LLDP messages

Command	Explanation
Global Mode	
lldp msgTxHold <*value*> **no lldp msgTxHold**	Configure the aging time multiplier of LLDP messages as the specified value or default value.

6. Configure the sending delay of updating messages

Command	Explanation
Global Mode	
lldp transmit delay <*seconds*> **no lldp transmit delay**	Configure the sending delay of updating messages as the specified value or default value.

7. Configure the intervals of sending Trap messages

Command	Explanation
Global Mode	
lldp notification interval <*seconds*> **no lldp notification interval**	Configure the intervals of sending Trap messages as the specified value or default value.

8. Configure to enable the Trap function of the port

Command	Explanation
Port Configuration Mode	
lldp trap <*enable*|*disable*>	Enable or disable the Trap function of the port.

9. Configure the optional information-sending attribute of the port

Command	Explanation
Port Configuration Mode	
lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] **no lldp transmit optional tlv**	Configure the optional information-sending attribute of the port as the option value of default values.

10. Configure the size of space to store Remote Table of the port

Command	Explanation
Port Configuration Mode	

lldp neighbors max-num < ***value*** **>** **no lldp neighbors max-num**	Configure the size of space to store Remote Table of the port as the specified value or default value.

11. Configure the type of operation when the Remote Table of the port is full

Command	Explanation
Port Configuration Mode	
lldp tooManyNeighbors {discard | delete}	Configure the type of operation when the Remote Table of the port is full.

12. Display and debug the relative information of LLDP

Command	Explanation
Admin, Global Mode	
show lldp	Display the current LLDP configuration information.
show lldp interface ethernet <*IFNAME*>	Display the LLDP configuration information of the current port.
show lldp traffic	Display the information of all kinds of counters.
show lldp neighbors interface ethernet < *IFNAME* >	Display the information of LLDP neighbors of the current port.
show debugging lldp	Display all ports with LLDP debug enabled.
Admin Mode	
debug lldp **no debug lldp**	Enable or disable the DEBUG switch.
debug lldp packets interface ethernet <*IFNAME*> **no debug lldp packets interface ethernet <*IFNAME*>**	Enable or disable the DEBUG packet-receiving and sending function in port or global mode.
Port configuration mode	
clear lldp remote-table	Clear Remote-table of the port.

5.3 LLDP Function Typical Example

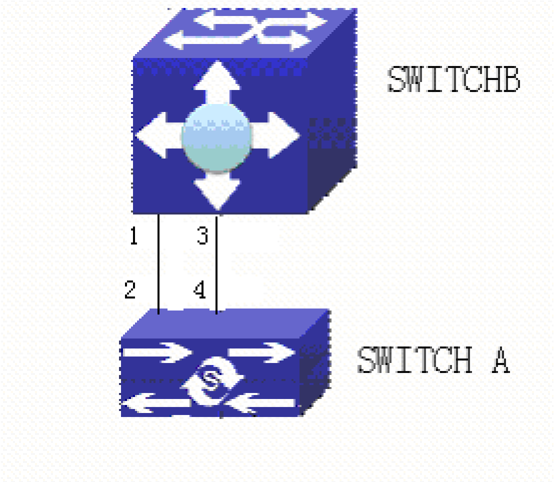

Fig 5-1 LLDP Function Typical Configuration Example

In the network topology graph above, the port 1,3 of SWITCH B are connected to port 2,4 of SWITCH A. Port 1 of SWITCH B is configured to message-receiving-only mode, Option TLV of port 4 of SWITCH A is configured as portDes and SysCap.

SWITCH A configuration task sequence:

```
SwitchA(config)# lldp enable
SwitchA(config)#interface ethernet 1/0/4
SwitchA(Config-If-Ethernet1/0/4)#lldp transmit optional tlv portDesc sysCap
SwitchA(Config-If-Ethernet1/0/4)exit
```

SWITCH B configuration task sequence:

```
SwitchB(config)#lldp enable
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)#lldp mode receive
SwitchB(Config-If-Ethernet1/0/1)#exit
```

5.4 LLDP Function Troubleshooting

☞ LLDP function is disabled by default. After enabling the global switch of LLDP, users can enable the debug switch “**debug lldp**” simultaneously to check debug information.

☞ Using “show” function of LLDP function can display the configuration information in global or port configuration mode.

Chapter 6 Port Channel Configuration

6.1 Introduction to Port Channel

To understand Port Channel, Port Group should be introduced first. Port Group is a group of physical ports in the configuration level; only physical ports in the Port Group can take part in link aggregation and become a member port of a Port Channel. Logically, Port Group is not a port but a port sequence. Under certain conditions, physical ports in a Port Group perform port aggregation to form a Port Channel that has all the properties of a logical port, therefore it becomes an independent logical port. Port aggregation is a process of logical abstraction to abstract a set of ports (port sequence) with the same properties to a logical port. Port Channel is a collection of physical ports and used logically as one physical port. Port Channel can be used as a normal port by the user, and can not only add network's bandwidth, but also provide link backup. Port aggregation is usually used when the switch is connected to routers, PCs or other switches.

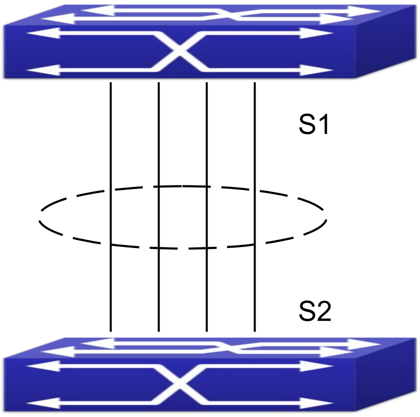

Fig 6-1 Port aggregation

As shown in the above, S1 is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from S1 needs to be transferred to S2 through the Port Channel, traffic allocation calculation will be performed based on the source MAC address and the lowest bit of target MAC address. The calculation result will decide which port to convey the traffic. If a port in Port Channel fails, the other ports will undertake traffic of that port through a traffic allocation algorithm. This algorithm is carried out by the hardware.

Switch offers two methods for configuring port aggregation: manual Port Channel creation and LACP (Link Aggregation Control Protocol) dynamic Port Channel creation. Port aggregation can only be performed on ports in full-duplex mode.

For Port Channel to work properly, member ports of the Port Channel must have the same properties as follows:

☞ All ports are in full-duplex mode.

☞ All Ports are of the same speed.

☞ All ports are Access ports and belong to the same VLAN or are all TRUNK ports, or are all Hybrid ports.

☞ If the ports are all TRUNK ports or Hybrid ports, then their “Allowed VLAN” and “Native VLAN” property should also be the same.

If Port Channel is configured manually or dynamically on switch, the system will automatically set the port with the smallest number to be Master Port of the Port Channel. If the spanning tree function is enabled in the switch, the spanning tree protocol will regard Port Channel as a logical port and send BPDU frames via the master port.

Port aggregation is closely related with switch hardware. Switch allow physical port aggregation of any two switches, maximum 128 groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. Switch have a built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical interface configuration mode.

6.2 Brief Introduction to LACP

LACP (Link Aggregation Control Protocol) is a kind of protocol based on IEEE802.3ad standard to implement the link dynamic aggregation. LACP protocol uses LACPDU (Link Aggregation Control Protocol Data Unit) to exchange the information with the other end.

After LACP protocol of the port is enabled, this port will send LACPDU to the other end to notify the system priority, the MAC address of the system, the priority of the port, the port ID and the operation Key. After the other end receives the information, the information is compared with the saving information of other ports to select the port which can be aggregated, accordingly, both sides can reach an agreement about the ports join or exit the dynamic aggregation group.

The operation Key is created by LACP protocol according to the combination of configuration (speed, duplex, basic configuration, management Key) of the ports to be aggregated.

After the dynamic aggregation port enables LACP protocol, the management Key is 0 by default. After the static aggregation port enables LACP, the management Key of the port is the same with the ID of the aggregation group.

For the dynamic aggregation group, the members of the same group have the same operation Key, for the static aggregation group, the ports of Active have the same operation Key.

The port aggregation is that multi-ports are aggregated to form an aggregation group, so as to implement the out/in load balance in each member port of the aggregation group and provides the better reliability.

6.2.1 Static LACP Aggregation

Static LACP aggregation is enforced by users configuration, and do not enable LACP protocol. When configuring static LACP aggregation, use “on” mode to force the port to enter the aggregation group.

6.2.2 Dynamic LACP Aggregation

1. The summary of the dynamic LACP aggregation

Dynamic LACP aggregation is an aggregation created/deleted by the system automatically, it does not allow the user to add or delete the member ports of the dynamic LACP aggregation. The ports which have the same attribute of speed and duplex, are connected to the same device, have the same basic configuration, can be dynamically aggregated together. Even if only one port can create the dynamic aggregation, that is the single port aggregation. In the dynamic aggregation, LACP protocol of the port is at the enable state.

2. The port state of the dynamic aggregation group

In dynamic aggregation group, the ports have two states: selected or standby. Both selected ports and standby ports can receive and send LACP protocol, but standby ports can not forward the data packets.

Because the limitation of the max port number in the aggregation group, if the current number of the member ports exceeds the limitation of the max port number, then the system of this end will negotiates with the other end to decide the port state according to the port ID. The negotiation steps are as follows:

Compare ID of the devices (the priority of the system + the MAC address of the system). First, compare the priority of the systems, if they are same, then compare the MAC address of the systems. The end with a small device ID has the high priority.

Compare the ID of the ports (the priority of the port + the ID of the port). For each port in the side of the device which has the high device priority, first, compare the priority of the ports, if the priorities are same, then compare the ID of the ports. The port with a small port ID is selected, and the others become the standby ports.

In an aggregation group, the port which has the smallest port ID and is at the selected state will be the master port, the other ports at the selected state will be the member port.

6.3 Port Channel Configuration Task List

1. Create a port group in Global Mode
2. Add ports to the specified group from the Port Mode of respective ports
3. Enter port-channel configuration mode
4. Set load-balance method for port-group
5. Set the system priority of LACP protocol

6. Set the port priority of the current port in LACP protocol
7. Set the timeout mode of the current port in LACP protocol

1. Creating a port group

Command	Explanation
Global Mode	
port-group <*port-group-number*> **no port-group <*port-group-number*>**	Create or delete a port group.

2. Add physical ports to the port group

Command	Explanation
Port Mode	
port-group <*port-group-number*> mode {active | passive | on} **no port-group**	Add the ports to the port group and set their mode.

3. Enter port-channel configuration mode.

Command	Explanation
Global Mode	
interface port-channel <*port-channel-number*>	Enter port-channel configuration mode.

4. Set load-balance method for port-group

Command	Explanation
Aggregation port configuration mode	
load-balance {src-mac **| dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip}**	Set load-balance for port-group.

5. Set the system priority of LACP protocol

Command	Explanation
Global mode	
lacp system-priority <*system-priority*> **no lacp system-priority**	Set the system priority of LACP protocol, the no command restores the default value.

6. Set the port priority of the current port in LACP protocol

Command	Explanation
Port mode	
lacp port-priority <*port-priority*> **no lacp port-priority**	Set the port priority in LACP protocol. The no command restores the default value.

7. Set the timeout mode of the current port in LACP protocol

Command	Explanation
Port mode	
lacp timeout {short | long} **no lacp timeout**	Set the timeout mode in LACP protocol. The no command restores the default value.

6.4 Port Channel Examples

Scenario 1: Configuring Port Channel in LACP.

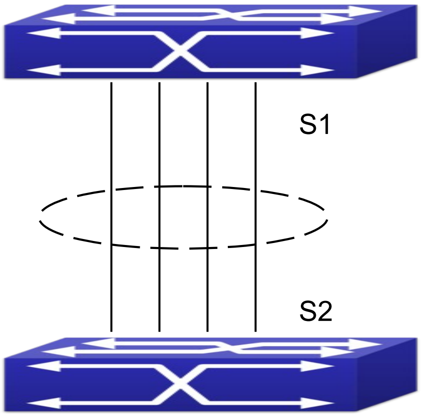

Fig 6-2 Configure Port Channel in LACP

The switches in the description below are all switch and as shown in the figure, ports 1, 2, 3, 4 of S1 are access ports and add them to group1 with active mode. Ports 6, 8, 9, 10 of S2 are access ports and add them to group2 with passive mode. All the ports should be connected with cables.

The configuration steps are listed below:

```
Switch1#config
Switch1(config)#interface ethernet 1/0/1-4
Switch1(Config-If-Port-Range)#port-group 1 mode active
```

```
Switch1(Config-If-Port-Range)#exit
Switch1(config)#interface port-channel 1
Switch1(Config-If-Port-Channel1)#

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode passive
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode passive
Switch2(Config-If-Port-Range)#exit
Switch2(config)#interface port-channel 2
Switch2(Config-If-Port-Channel2)#
```

Configuration result:

Shell prompts ports aggregated successfully after a while, now ports 1, 2, 3, 4 of S1 form an aggregated port named “Port-Channel1”, ports 6, 8, 9, 10 of S2 form an aggregated port named “Port-Channel2”; can be configured in their respective aggregated port mode.

Scenario 2: Configuring Port Channel in ON mode.

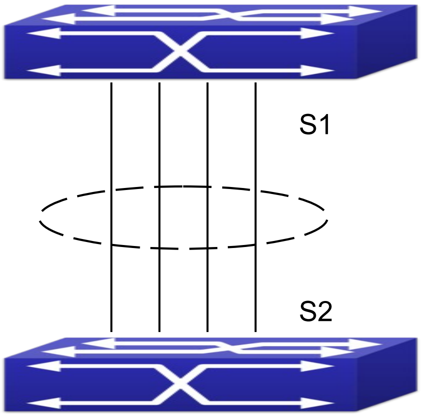

Fig 6-3 Configure Port Channel in ON mode

As shown in the figure, ports 1, 2, 3, 4 of S1 are access ports and add them to group1 with “on” mode. Ports 6, 8, 9, 10 of S2 are access ports and add them to group2 with “on” mode.

The configuration steps are listed below:

```
Switch1#config
Switch1(config)#interface ethernet 1/0/1
Switch1(Config-If-Ethernet1/0/1)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/1)#exit
```

```
Switch1(config)#interface ethernet 1/0/2
Switch1 (Config-If-Ethernet1/0/2)#port-group 1 mode on
Switch1 (Config-If-Ethernet1/0/2)#exit
Switch1 (config)#interface ethernet 1/0/3
Switch1 (Config-If-Ethernet1/0/3)#port-group 1 mode on
Switch1 (Config-If-Ethernet1/0/3)#exit
Switch1 (config)#interface ethernet 1/0/4
Switch1 (Config-If-Ethernet1/0/4)#port-group 1 mode on
Switch1 (Config-If-Ethernet1/0/4)#exit

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2 (Config-If-Ethernet1/0/6)#port-group 2 mode on
Switch2 (Config-If-Ethernet1/0/6)#exit
Switch2 (config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode on
Switch2(Config-If-Port-Range)#exit
```

Configuration result:

Add ports 1, 2, 3, 4 of S1 to port-group1 in order, and we can see a group in “on” mode is completely joined forcedly, switch in other ends won’t exchange LACP PDU to complete aggregation. Aggregation finishes immediately when the command to add port 1/0/2 to port-group 1 is entered, port 1 and port 2 aggregate to be port-channel 1, when port 1/0/3 joins port-group 1, port-channel 1 of port 1 and 2 are ungrouped and re-aggregate with port 3 to form port-channel 1, when port 1/0/4 joins port-group 1, port-channel 1 of port 1, 2 and 3 are ungrouped and re-aggregate with port 4 to form port-channel 1. (It should be noted that whenever a new port joins in an aggregated port group, the group will be ungrouped first and re-aggregated to form a new group.) Now all four ports in both S1 and S2 are aggregated in “on” mode and become an aggregated port respectively.

6.5 Port Channel Troubleshooting

If problems occur when configuring port aggregation, please first check the following for causes.

☞ Ensure all ports in a port group have the same properties, i.e., whether they are in full-duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make corrections.

☞ Some commands cannot be used on a port in port-channel, such as arp, bandwidth, ip, ip-forward, etc.

Chapter 7 MTU Configuration

7.1 Introduction to MTU

So far the Jumbo (Jumbo Frame) has not reach a determined standard in the industry (including the format and length of the frame). Normally frames sized within 1519-12000 should be considered jumbo frame. Networks with jumbo frames will increase the speed of the whole network by 2% to 5%. Technically the Jumbo is just a lengthened frame sent and received by the switch. However considering the length of Jumbo frames, they will not be sent to CPU. We discard the Jumbo frames sent to CPU in the packet receiving process.

7.2 MTU Configuration Task Sequence

1. Configure enable MTU function

1. Configure enable MTU function

Command	Explanation
Global Mode	
mtu [<mtu-value>] **no mtu enable**	Enable the receiving/sending function of MTU frame. The no command disables sending and receiving function of MTU frames.

Chapter 8 bpdu-tunnel Configuration

8.1 Introduction to bpdu-tunnel

BPDU Tunnel is a Layer 2 tunnel technology. It allows Layer 2 protocol packets of geographically dispersed private network users to be transparently transmitted over specific tunnels across a service provider network.

8.1.1 bpdu-tunnel function

In MAN application, multi-branches of a corporation may connect with each other by the service provider network. VPN provided by the service provider enables the geographically dispersed networks to form a local LAN, so the service provider needs to provide the tunnel function, namely, data information generated by user's network is able to inextenso arrive at other networks of the same corporation through the service provider network. To maintain a local concept, it not only needs to transmit the data within the user's private network across the tunnel, but also transmit layer 2 protocol packets within the user's private network.

8.1.2 Background of bpdu-tunnel

Special lines are used in a service provider network to build user-specific Layer 2 networks. As a result, a user network is broken down into parts located at different sides of the service provider network. As shown in Figure, User A has two devices (CE 1 and CE 2) and both devices belong to the same VLAN. User's network is divided into network 1 and network 2, which are connected by the service provider network. When Layer 2 protocol packets cannot implement the passthrough across the service provider network, the user's network cannot process independent Layer 2 protocol calculation (for example, spanning tree calculation), so they affect each other.

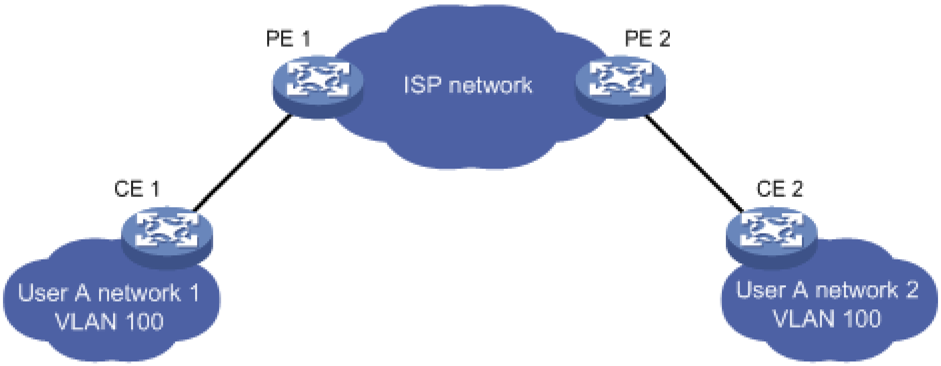

Fig 8-1 BPDU Tunnel application

8.2 bpdu-tunnel Configuration Task List

bpdu-tunnel configuration task list:
1. Configure tunnel MAC address globally
2. Configure the port to support the tunnel

1. Configure tunnel MAC address globally

Command	Explanation
Global mode	
bpdu-tunnel dmac <mac> **no bpdu-tunnel dmac**	Configure or cancel the tunnel MAC address globally.

2. Configure the port to support the tunnel

Command	Explanation
Port mode	

bpdu-tunnel {stp|gvrp|uldp|lacp|dot1x}
no bpdu-tunnel {stp|gvrp|uldp|lacp|dot1x}
	Enable the port to support the tunnel, the no command disables the function.

8.3 Examples of bpdu-tunnel

Special lines are used in a service provider network to build user-specific Layer 2 networks. As a result, a user network is broken down into parts located at different sides of the service provider network. As shown in Figure, User A has two devices (CE 1 and CE 2) and both devices belong to the same VLAN. User's network is divided into network 1 and network 2, which are connected by the service provider network. When Layer 2 protocol packets cannot implement the passthrough across the service provider network, the user's network cannot process independent Layer 2 protocol calculation (for example, spanning tree calculation), so they affect each other.

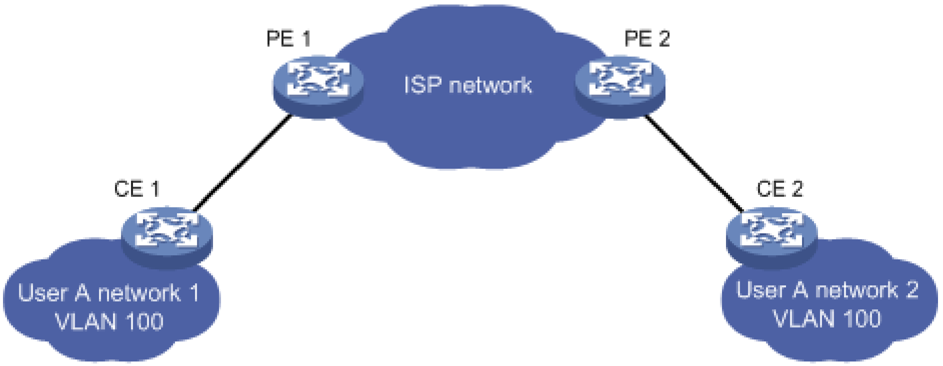

Fig 8-2 BPDU Tunnel application environment

With BPDU Tunnel, Layer 2 protocol packets from user's networks can be passed through over the service provider network in the following work flow:

1. After receiving a Layer 2 protocol packet from network 1 of user A, PE 1 in the service provider network encapsulates the packet, replaces its destination MAC address with a specific multicast MAC address, and then forwards the packet in the service provider network.

2. The encapsulated Layer 2 protocol packet (called BPDU Tunnel packet) is forwarded to PE 2 at the other end of the service provider network, which de-encapsulates the packet, restores the original destination MAC address of the packet, and then sends the packet to network 2 of user A.

bpdu-tunnel configuration of edge switches PE1 and PE2 in the following:

PE1 configuration:

```
PE1(config)# bpdu-tunnel dmac 01-02-03-04-05-06
PE1(config-if-ethernet1/0/1)# bpdu-tunnel stp
PE1(config-if-etherne1/0/1)# bpdu-tunnel lacp
PE1(config-if-ethernet1/0/1)# bpdu-tunnel uldp
PE1(config-if-ethernet1/0/1)# bpdu-tunnel gvrp
PE1(config-if-ethernet1/0/1)# bpdu-tunnel dot1x
```

PE2 configuration:

```
PE2(config)# bpdu-tunnel dmac 01-02-03-04-05-06
PE2(config-if-ethernet1/0/1)# bpdu-tunnel stp
PE2(config-if-ethernet1/0/1)# bpdu-tunnel lacp
PE2(config-if-ethernet1/0/1)# bpdu-tunnel uldp
PE2(config-if-ethernet1/0/1)# bpdu-tunnel gvrp
PE2(config-if-ethernet1/0/1)# bpdu-tunnel dot1x
```

8.4 bpdu-tunnel Troubleshooting

After port disables stp, gvrp, uldp, lacp and dot1x functions, it is able to configure bpdu-tunnel function.

Chapter 9 DDM Configuration

9.1 Introduction to DDM

9.1.1 Brief Introduction to DDM

DDM (Digital Diagnostic Monitor) makes the detailed digital diagnostic function standard in SFF-8472 MSA. It set that the parameter signal is monitored and make it to digitize on the circuit board of the inner module. After that, providing the demarcated result or the digitize measure result and the demarcate parameter which are saved in the standard memory framework, so as to expediently read by serial interface with double cables.

Normally, intelligent fiber modules support Digital Diagnostic function. Network management units is able to monitor the parameters (temperature, voltage, bias current, tx power and rx power) of the fiber module to obtain theirs thresholds and the real-time state of the current fiber module by the inner MCU of the fiber module. That is able to help the network management units to locate the fault in the fiber link, reduce the maintenance workload and enhance the system reliability.

DDM applications are shown in the following:

1. Module lifetime forecast

Monitoring the bias current is able to forecast the laser lifetime. Administrator is able to find some potential problems by monitoring voltage and temperature of the module.

（1）High Vcc voltage will result in the breakdown CMOS, low Vcc voltage will result in the abnormity work.

（2）High rx power will damage the receiving module, low rx power will result that the receiving module cannot work normally.

（3）High temperature will result in the fast aging of the hardware.

（4）Monitoring the received fiber power to monitor the capability of the link and the remote switch.

2. Fault location

In fiber link, locating the fault is important to the fast overload of the service, fault isolation is able to help administrator to fast locate the location of the link fault within the module (local module or remote module) or on the link, it also reduce the time for restoring the fault of the system.

Analyzing warning and alarm status of real-time parameters (temperature, voltage, bias current, tx power and rx power) can fast locate the fault through Digital Diagnostic function. Besides, the state of Tx Fault and Rx LOS is important for analyzing the fault.

3. Compatibility verification

Compatibility verification is used to analyze whether the environment of the module

accords the data manual or it is compatible with the corresponding standard, because the module capability is able to be ensured only in the compatible environment. Sometimes, environment parameters exceed the data manual or the corresponding standard, it will make the falling of the module capability that result in the transmission error.
Environment is not compatible with the module are as below:
（1）Voltage exceeds the set range
（2）Rx power is overload or is under the sensitivity of the transceiver
（3）Temperature exceeds the range of the running temperature

9.1.2 DDM Function

DDM descriptions are shown in the following:
1. Show the monitoring information of the transceiver

Administrator is able to know the current working state of the transceiver and find some potential problems through checking the real-time parameters (including TX power, RX power, Temperature, Voltage, Bias current) and querying the monitoring information (such as warning, alarm, real-time state and threshold, and so on). Besides, checking the fault information of the fiber module helps administrator to fast locate the link fault and saves the restored time.

2. Threshold defined by the user

For real-time parameters (TX power, RX power, Temperature, Voltage, Bias current), there are fixed thresholds. Because the user's environments are difference, the users is able to define the threshold (including high alarm, low alarm, high warn, low warn) to flexibly monitor the working state of the transceiver and find the fault directly.

The thresholds configured by the user and the manufacturer can be shown at the same time. When the threshold defined by the user is irrational, it will prompt the user and automatically process alarm or warning according to the default threshold. (the user is able to restore all thresholds to the default thresholds or restore a threshold to the default threshold)

Threshold rationality: high/low warn should be between high alarm and low alarm and high threshold should be higher than low threshold, namely, high alarm>= high warn>= low warn>= low alarm.

For fiber module, verification mode of the receiving power includes inner verification and outer verification which are decided by the manufacturer. Besides the verification mode of the real-time parameters and the default thresholds are same.

3. Transceiver monitoring

Besides checking the real-time working state of the transceiver, the user needs to monitor the detailed status, such as the former abnormity time and the abnormity type. Transceiver monitoring helps the user to find the former abnormity status through checking the log and query the last abnormity status through executing the commands. When the user finds the abnormity information of the fiber module, the fiber module information may be remonitored after processing the abnormity information, here, the user is able to know the abnormity information and renew the monitoring.

9.2 DDM Configuration Task List

DDM configuration task list:

1. Show the real-time monitoring information of the transceiver
2. Configure the alarm or warning thresholds of each parameter for the transceiver
3. Configure the state of the transceiver monitoring

（1） Configure the interval of the transceiver monitoring
（2） Configure the enable state of the transceiver monitoring
（3） Show the information of the transceiver monitoring
（4） Clear the information of the transceiver monitoring

1. Show the real-time monitoring information of the transceiver

Command	Explanation
User mode, admin mode and global mode	
show transceiver [interface ethernet <interface-list>][detail]	Show the monitoring of the transceiver.

2. Configure the alarm or warning thresholds of each parameter for the transceiver

Command	Explanation
Port mode	
transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}	Set the threshold defined by the user.

3. Configure the state of the transceiver monitoring

(1) Configure the interval of the transceiver monitoring

Command	Explanation
Global mode	
transceiver-monitoring interval <minutes> **no transceiver-monitoring interval**	Set the interval of the transceiver monitor. The no command sets the interval to be the default interval of 15 minutes.

（2）Configure the enable state of the transceiver monitoring

Command	Explanation
Port mode	
transceiver-monitoring {enable | disable}	Set whether the transceiver monitoring is enabled. Only the port enables the transceiver monitoring, the system records the abnormity state. After the port disables the function, the abnormity information will be clear.

（3）Show the information of the transceiver monitoring

Command	Explanation
Admin mode and global mode	
show transceiver threshold-violation [interface ethernet <interface-list>]	Show the information of the transceiver monitoring, including the last threshold-violation informatijon, the interval of the current transceiver monitoring and whether the port enables the transceiver monitoring.

（4）Clear the information of the transceiver monitoring

Command	Explanation
Admin mode	
clear transceiver threshold-violation [interface ethernet <interface-list>]	Clear the threshold violation of the transceiver monitor.

9.3 Examples of DDM

Example1:

Ethernet 21 and Ethernet 23 are inserted the fiber module with DDM, Ethernet 24 is inserted the fiber module without DDM, Ethernet 22 does not insert any fiber module, show the DDM information of the fiber module.

a、 Show the information of all interfaces which can read the real-time parameters normally,(No fiber module is inserted or the fiber module is not supported, the information will not be shown), for example:

```
Switch#show transceiver
Interface   Temp（℃） Voltage（V） Bias（mA）  RX Power（dBM）     TX
Power（dBM）
1/0/21    33       3.31        6.11       -30.54(A-)       -6.01
1/0/23    33       5.00（W+） 6.11       -20.54(W-)       -6.02
```

b、Show the information of the specified interface. (N/A means no fiber module is inserted or does not support the fiber module), for example:

```
Switch#show transceiver interface ethernet 1/0/21-22;23
Interface   Temp（℃） Voltage（V） Bias（mA）  RX Power（dBM）     TX
Power（dBM）
1/0/21    33       3.31        6.11       -30.54(A-)      -6.01
1/0/22    N/A      N/A         N/A        N/A             N/A
1/0/23    33       5.00（W+） 6.11       -20.54(W-)      -6.02
```

c、Show the detailed information, including base information, parameter value of the real-time monitoring, warning, alarm, abnormity state and threshold information, for example:

```
Switch#show transceiver interface ethernet 1/0/21-22;24 detail
Ethernet 1/0/21 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX, Link length is 550 m for 50um Multi-Mode Fiber.
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
Brief alarm information:
RX loss of signal
Voltage high
RX power low
Detail diagnostic and threshold information:
            Diagnostic               Threshold
                  Realtime Value   High Alarm  Low Alarm   High Warn    Low Warn
                    --------------    -----------   -----------    ------------    ---------
Temperature（℃） 33          70        0          70         0
Voltage（V）      7.31(A+)     5.00      0.00       5.00        0.00
Bias current（mA） 6.11(W+)      10.30     0.00       5.00        0.00
RX Power（dBM）   -30.54(A-)    9.00      -25.00     9.00        -25.00
TX Power（dBM）   -6.01         9.00      -25.00     9.00        -25.00

Ethernet 1/0/22 transceiver detail information: N/A

Ethernet 1/0/24 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX, Link length is 550 m for 50um Multi-Mode Fiber.
```

```
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
Brief alarm information: N/A
Detail diagnostic and threshold information: N/A
```

Example2:

Ethernet 21 is inserted the fiber module with DDM. Configure the threshold of the fiber module after showing the DDM information.

Step1: Show the detailed DDM information.

```
Switch#show transceiver interface ethernet 1/0/21 detail
Ethernet 1/0/21 transceiver detail information:
Base information:
……
Brief alarm information:
RX loss of signal
Voltage high
RX power low
Detail diagnostic and threshold information:
              Diagnostic                Threshold
                    Realtime Value   High Alarm  Low Alarm   High Warn   Low Warn
                     --------------      -----------    -----------     ------------     ---------
Temperature（℃）   33            70        0         70       0
Voltage（V）       7.31(A+)        5.00      0.00       5.00      0.00
Bias current（mA） 6.11(W+)         10.30     0.00       5.00      0.00
RX Power（dBM）   -30.54(A-)        9.00     -25.00      9.00      -25.00
TX Power（dBM）   -13.01           9.00     -25.00      9.00      -25.00
```

Step2: Configure the tx-power threshold of the fiber module, the low-warning threshold is -12, the low-alarm threshold is -10.00.

```
Switch#config
Switch(config)#interface ethernet 1/0/21
Switch(config-if-ethernet1/0/21)#transceiver threshold tx-power low-warning -12
Switch(config-if-ethernet1/0/21)#transceiver threshold tx-power low-alarm -10.00
```

Step3: Show the detailed DDM information of the fiber module. The alarm uses the threshold configured by the user, the threshold configured by the manufacturer is labeled with the bracket. There is the alarm with 'A-' due to -13.01 is less than -12.00.

```
Switch#show transceiver interface ethernet 1/0/21 detail
Ethernet 1/0/21 transceiver detail information:
Base information:
……
Brief alarm information:
RX loss of signal
Voltage high
```

```
RX power low
TX power low
Detail diagnostic and threshold information:
              Diagnostic                  Threshold
                    Realtime Value   High Alarm  Low Alarm   High Warn   Low Warn
                     --------------      -----------    -----------      ----------     ---------
Temperature（℃）  33          70         0         70        0
Voltage（V）      7.31(A+)      5.00       0.00       5.00       0.00
Bias current（mA） 6.11(W+)      10.30      0.00        5.00       0.00
RX Power（dBM）  -30.54(A-)      9.00      -25.00       9.00       -25.00
TX Power（dBM）  -13.01(A-)      9.00     -12.00(-25.00)  9.00    -10.00(-25.00)
```

Example3:

Ethernet 21 is inserted the fiber module with DDM. Enable the transceiver monitoring of the port after showing the transceiver monitoring of the fiber module.

Step1: Show the transceiver monitoring of the fiber module. Both ethernet 21 and ethernet 22 do not enable the transceiver monitoring, its interval is set to 30 minutes.

```
Switch(config)#show transceiver threshold-violation interface ethernet 1/0/21-22
Ethernet 1/0/21 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn’t exist.

Ethernet 1/0/22 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn’t exist.
```

Step2: Enable the transceiver monitoring of ethernet 21.

```
Switch(config)#interface ethernet 1/0/21
Switch(config-if-ethernet1/0/21)#transceiver-monitoring enable
```

Step3: Show the transceiver monitoring of the fiber module. In the following configuration, ethernet 21 enabled the transceiver monitoring, the last threshold-violation time is Jan 02 11:00:50 2011, the detailed DDM information exceeding the threshold is also shown.

```
Switch(config-if-ethernet1/0/21)#quit
Switch(config)#show transceiver threshold-violation interface ethernet 1/0/21-22
Ethernet 1/0/21 transceiver threshold-violation information:
Transceiver monitor is enabled. Monitor interval is set to 30 minutes.
The current time is Jan 02 12:30:50 2011.
The last threshold-violation time is Jan 02 11:00:50 2011.
Brief alarm information:
RX loss of signal
RX power low
Detail diagnostic and threshold information:
              Diagnostic                  Threshold
              Realtime Value  High Alarm     Low Alarm     High Warn     Low Warn
                ------------     -----------       -----------       ------------       ---------
Temperature（℃）  33        70         0            70           0
Voltage（V）       7.31      10.00       0.00         5.00          0.00
Bias current（mA） 3.11      10.30       0.00          5.00          0.00
RX Power（dBM） -30.54(A-)  9.00       -25.00(-34)    9.00          -25.00
TX Power（dBM）  -1.01      9.00       -12.05        9.00          -10.00

Ethernet 1/0/22 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn’t exist.
```

9.4 DDM Troubleshooting

If problems occur when configuring DDM, please check whether the problem is caused by the following reasons:

- Ensure that the transceiver of the fiber module has been inserted fast on the port, or else DDM configuration will not be shown.
- Ensure that SNMP configuration is valid, or else the warning event cannot inform the network management system.
- Because only some boards and box switches support SFP with DDM or XFP with DDM, ensure the used board and switch support the corresponding function.
- When using **show transceiver** command or **show transceiver detail** command, it cost much time due to the switch will check all ports, so it is recommended to query the monitoring information of the transceiver on the specified port.
- Ensure the threshold defined by the user is valid. When any threshold is error, the transceiver will give an alarm according to the default setting automatically.
- The DDM information of QSFP+ port does not support transmission power (TX power), it is determined by SFF-8436.
- If QSFP+ port is configured as 40G mode, it will show the DDM information of all 4 channels; if it is configured as 4x10G mode, it only shows the channel information related to the current 10G port.
- DAC wire has optical module itself, if the wire is passive mode, there is no DDM information; if the wire is active mode, DDM information can be viewed.

Chapter 10 EFM OAM Configuration

10.1 Introduction to EFM OAM

Ethernet is designed for Local Area Network at the beginning, but link length and network scope is extended rapidly while Ethernet is also applied to Metropolitan Area Network and Wide Area Network along with development. Due to lack the effectively management mechanism, it affects Ethernet application to Metropolitan Area Network and Wide Area Network, implementing OAM on Ethernet becomes a necessary development trend.

There are four protocol standards about Ethernet OAM, they are 802.3ah (EFM OAM), 802.3ag (CFM), E-LMI and Y.1731. EFM OAM and CFM are set for IEEE organization. EFM OAM works in data link layer to validly discover and manage the data link status of rock-bottom. Using EFM OAM can effectively advance management and maintenance for Ethernet to ensure the stable network operation. CFM is used for monitoring the whole network connectivity and locating the fault in access aggregation network layer. Compare with CFM, Y.1731 standard set by ITU (International Telecommunications Union) is more powerful. E-LMI standard set by MEF is only applied to UNI. So above protocols can be used to different network topology and management, between them exist the complementary relation.

EFM OAM (Ethernet in the First Mile Operation, Administration and Maintenance) works in data link layer of OSI model to implement the relative functions through OAM sublayer, figure is as bleow:

Fig 10-1 OAM location in OSI model

OAM protocol data units (OAMPDU) use destination MAC address 01-80-c2-00-00-02 of protocol, the max transmission rate is 10Pkt/s.

EFM OAM is established on the basis of OAM connection, it provides a link operation management mechanism such as link monitoring, remote fault detection and remote loopback testing, the simple introduction for EFM OAM in the following:

1. Ethernet OAM connection establishment

Ethernet OAM entity discovers remote OAM entities and establishes sessions with them by exchanging Information OAMPDUs. EFM OAM can operate in two modes: active mode and passive mode. One session can only be established by the OAM entity working in the active mode and ones working in the passive mode need to wait until it receives the connection request. After an Ethernet OAM connection is established, the Ethernet OAM entities on both sides exchange Information OAMPDUs continuously to keep the valid Ethernet OAM connection. If an Ethernet OAM entity receives no Information OAMPDU for five seconds, the Ethernet OAM connection is disconnected.

2. Link Monitoring

Fault detection in an Ethernet is difficult, especially when the physical connection in the network is not disconnected but network performance is degrading gradually. Link monitoring is used to detect and discover link faults in various environments. EFM OAM implements link monitoring through the exchange of Event Notification OAMPDUs. When detecting a link error event, the local OAM entity sends an Event Notification OAMPDU to notify the remote OAM entity. At the same time it will log information and send SNMP Trap to the network management system. While OAM entity on the other side receives the notification, it will also log and report it. With the log information, network administrators can keep track of network status in time.

The link event monitored by EFM OAM means that the link happens the error event, including Errored symbol period event, Errored frame event, Errored frame period event, Errored frame seconds event.

Errored symbol period event: The errored symbol number can not be less than the low threshold. (Symbol: the min data transmission unit of physical medium. It is unique for coding system, the symbols may be different for different physical mediums, symbol rate means the changed time of electron status per second.)

Errored frame period event: Specifying N is frame period, the errored frame number within the period of receiving N frames can not be less than the low threshold. (Errored frame: Receiving the errored frame detected by CRC.)

Errored frame event: The number of detected error frames over M seconds can not be less than the low threshold.

Errored frame seconds event: The number of error frame seconds detected over M seconds can not be less than the low threshold. (Errored frame second: Receiving an errored frame at least in a second.)

3. Remote Fault Detection

In a network where traffic is interrupted due to device failures or unavailability, the flag field defined in Ethernet OAMPDUs allows an Ethernet OAM entity to send fault information to its peer. As Information OAMPDUs are exchanged continuously across established OAM connections, an Ethernet OAM entity can inform one of its OAM peers of link faults through Information OAMPDUs. Therefore, the network administrator can keep track of link status in time through the log information and troubleshoot in time.

There are three kinds of link faults for Information OAMPDU, they are Critical Event, Dying Gasp and Link Fault, and their definitions are different for each manufacturer, here the definitions are as below:

Critical Event: EFM OAM function of port is disabled.

Link Fault: The number of unidirectional operation or fault can not be less than the high threshold in local. Unidirectional Operation means unidirectional link can not work normally on full-duplex link without autonegotiaction. EFM OAM can detect the fault and inform the remote OAM peers through sending Information OAMPDU.

Dying Gasp: There is no definition present. Although device does not generate Dying Gasp OAMPDU, it still receives and processes such OAMPDU sent by its peer.

Typical EFM OAM application topology is in the following, it is used for point-to-point link and emulational IEEE 802.3 point-to-point link. Device enables EFM OAM through point-to-point connection to monitor the link fault in the First Mile with Ethernet access. For user, the connection between user to telecommunication is “the First Mile”, for service provider, it is “the Last Mile”.

Fig 10-2 Typical OAM application topology

10.2 EFM OAM Configuration

EFM OAM configuration task list

1. Enable EFM OAM function of port
2. Configure link monitor
3. Configure remote failure
4. Enable EFM OAM loopback of port

Note: it needs to enable OAM first when configuring OAM parameters.

1. Enable EFM OAM function of port

Command	Explanation
Port mode	
ethernet-oam mode {active | passive}	Configure work mode of EFM OAM, default is active mode.
ethernet-oam **no ethernet-oam**	Enable EFM OAM of port, no command disables EFM OAM of port.
ethernet-oam period <seconds> **no ethernet-oam period**	Configure transmission period of OAMPDU (optional), no command restores the default value.
ethernet-oam timeout <seconds> **no ethernet-oam timeout**	Configure timeout of EFM OAM connection, no command restores the default value.

2. Configure link monitor

Command	Explanation
Port mode	
ethernet-oam link-monitor **no ethernet-oam link-monitor**	Enable link monitor of EFM OAM, no command disables link monitor.

ethernet-oam errored-symbol-period {threshold low <low-symbols> | window <seconds>}
no ethernet-oam errored-symbol-period {threshold low | window }
	Configure the low threshold and window period of errored symbol period event, no command resotores the default value. (optional)

ethernet-oam errored-frame-period {threshold low <low-frames> | window <seconds>}
no ethernet-oam errored-frame-period {threshold low | window }
	Configure the low threshold and window period of errored frame period event, no command resotores the default value.

ethernet-oam errored-frame {threshold low <low-frames> | window <seconds>}
no ethernet-oam errored-frame {threshold low | window }
	Configure the low threshold and window period of errored frame event, no command resotores the default value. (optional)

ethernet-oam errored-frame-seconds {threshold low <low-frame-seconds> | window <seconds>}
no ethernet-oam errored-frame-seconds {threshold low | window }
	Configure the low threshold and window period of errored frame seconds event, no command resotores the default value. (optional)

3. Configure remote failure

Command	Explanation
Port mode	
ethernet-oam remote-failure **no ethernet-oam remote-failure**	Enable remote failure detection of EFM OAM (failure means critical-event or link-fault event of the local), no command disables the function. (optional)
ethernet-oam errored-symbol-period threshold high {high-symbols | none} **no ethernet-oam errored-symbol-period threshold high**	Configure the high threshold of errored symbol period event, no command restores the default value. (optional)
ethernet-oam errored-frame-period threshold high {high-frames | none} **no ethernet-oam errored-frame-period threshold high**	Configure the high threshold of errored frame period event, no command restores the default value. (optional)
ethernet-oam errored-frame threshold high {high-frames | none} **no ethernet-oam errored-frame threshold high**	Configure the high threshold of errored frame event, no command restores the default value. (optional)
ethernet-oam errored-frame-seconds threshold high {high-frame-seconds | none} **no ethernet-oam errored-frame-seconds threshold high**	Configure the high threshold of errored frame seconds event, no command restores the default value. (optional)

4. Enable EFM OAM loopback of port

Command	Explanation
Port mode	
ethernet-oam remote-loopback **no ethernet-oam remote-loopback**	Enable remote EFM OAM entity to enter OAM loopback mode (its peer needs to configure OAM loopback supporting), no command cancels remote OAM loopback.

10.3 EFM OAM Example

Example:

CE and PE devices with point-to-point link enable EFM OAM to monitor "the First Mile" link performance. It will report the log information to network management system.

Fig 10-3 Typical OAM application topology

Configuration procedure: (Omitting SNMP and Log configuration in the following)

Configuration on CE:

```
CE(config)#interface ethernet1/0/1
CE (config-if-ethernet1/0/1)#ethernet-oam mode passive
CE (config-if-ethernet1/0/1)#ethernet-oam
```

Other parameters use the default configuration.

Configuration on PE:

```
PE(config)#interface ethernet 1/0/1
PE (config-if-ethernet1/0/1)#ethernet-oam
```

Other parameters use the default configuration.

Execute the following command when using remote loopback.

```
PE(config-if-ethernet1/0/1)#ethernet-oam remote-loopback
```

Execute the following command to make one of OAM peers exiting OAM loopback after complete detection.

```
PE(config-if-ethernet1/0/1)# no ethernet-oam remote-loopback
```

10.4 EFM OAM Troubleshooting

When using EFM OAM, it occurs the problem, please check whether the problem is resulted by the following reasons:

☞ Check whether OAM entities of two peers of link in passive mode. If so, EFM OAM connection can not be established between two OAM entities.

☞ Ensuring SNMP configuration is correct, or else errored event can not be reported to network management system.

☞ Link does not normally communicate in OAM loopback mode, it should cancel remote loopback in time after detect the link performance.

☞Ensuring the used board supports remote loopback function.

☞Port should not configure STP, MRPP, ULPP, Flow Control, loopback detection functions after it enables OAM loopback function, because OAM remote loopback function and these functions are mutually exclusive.

Chapter 11 LLDP-MED

11.1 Introduction to LLDP-MED

LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) based on 802.1AB LLDP (Link Layer Discovery Protocol) of IEEE. LLDP provides a standard link layer discovery mode, it sends local device information (including its major capability, management IP address, device ID and port ID) as TLV (type/length/value) triplets in LLDPDU (Link Layer Discovery Protocol Data Unit) to the direct connection neighbors. The device information received by the neighbors will be stored with a standard management information base (MIB). This allows a network management system to quickly detect and identify the communication status of the link.

In 802.1AB LLDP, there is no transmission and management about the voice device information. To deploy and manage voice device expediently, LLDP-MED TLVs provide multiple information, such as PoE (Power over Ethernet), network policy, and the location information of the emergent telephone service.

11.2 LLDP-MED Configuration Task Sequence

1. Basic LLDP-MED configuration

Command	Explanation
Port mode	
lldp transmit med tlv all **no lldp transmit med tlv all**	Configure the specified port to send all LLDP-MED TLVs. The no command disables the function.
lldp transmit med tlv capability **no lldp transmit med tlv capability**	Configure the specified port to send LLDP-MED Capability TLV. The no command disables the capability.
lldp transmit med tlv networkPolicy **no lldp transmit med tlv networkPolicy**	Configure the specified port to send LLDP-MED Network Policy TLV. The no command disables the capability.
lldp transmit med tlv extendPoe **no lldp transmit med tlv extendPoe**	Configure the specified port to send LLDP-MED Extended Power-Via-MDI TLV. The no command disables the capability.

lldp transmit med tlv inventory **no lldp transmit med tlv inventory**	Configure the port to send LLDP-MED Inventory Management TLVs. The no command disables the capability.
network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [status {enable | disable}] [tag {tagged | untagged}] [vid {<*vlan-id*> | dot1p}] [cos <*cos-value*>] [dscp <*dscp-value*>] **no network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming- video | video-signaling}**	Configure network policy of the port, including VLAN ID, the supported application (such as voice and video), the application priority and the used policy, and so on.
civic location {dhcp server | switch | endpointDev} <*country-code*> **no civic location**	Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode. The no command cancels all configurations of the location with Civic Address LCI format.
ecs location <*tel-number*> **no ecs location**	Configure the location with ECS ELIN format on the port, the no command cancels the configured location.
lldp med trap {enable | disable}	Enable or disable LLDP-MED trap for the specified port.
Civic Address LCI address mode	
{description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} <*address*> **no {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}**	Configure the detailed address after enter Civic Address LCI address mode of the port.
Global mode	
lldp med fast count <*value*> **no lldp med fast count**	When the fast LLDP-MED startup mechanism is enabled, it needs to fast send the LLDP packets with LLDP-MED TLV, this command is

	used to set the value of the fast sending packets, the no command restores the default value.
Admin mode	
show lldp	Show the configuration of the global LLDP and LLDP-MED.
show lldp [interface ethernet <*IFNAME*>]	Show the configuration of LLDP and LLDP-MED on the current port.
show lldp neighbors [interface ethernet <*IFNAME*>]	Show LLDP and LLDP-MED configuration of the neighbors.

11.3 LLDP-MED Example

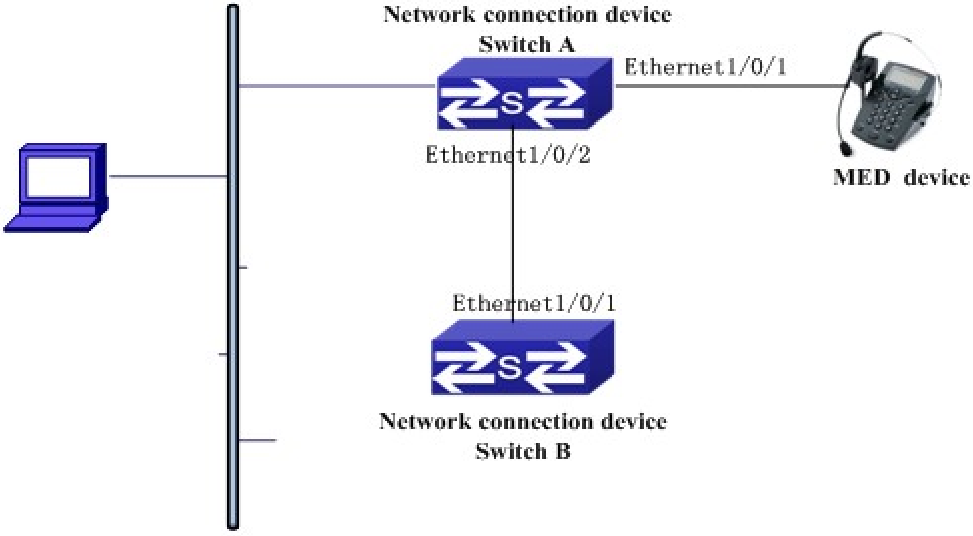

Fig 11-1 Basic LLDP-MED configuration topology

1) Configure Switch A

```
SwitchA(config)#interface ethernet1/0/1
SwitchA (Config-If-Ethernet1/0/1)# lldp enable
SwitchA (Config-If-Ethernet1/0/1)# lldp mode both（this configuration can be omitted, the default mode is RxTx）
SwitchA (Config-If-Ethernet1/0/1)# lldp transmit med tlv capability
SwitchA (Config-If-Ethernet1/0/1)# lldp transmit med tlv network policy
SwitchA (Config-If-Ethernet1/0/1)# lldp transmit med tlv inventory
SwitchB (Config-If-Ethernet1/0/1)# network policy voice tag tagged vid 10 cos 5 dscp 15
SwitchA (Config-If-Ethernet1/0/1)# exit
SwitchA (config)#interface ethernet1/0/2
SwitchA (Config-If-Ethernet1/0/2)# lldp enable
SwitchA (Config-If-Ethernet1/0/2)# lldp mode both
```

2) Configure Switch B

```
SwitchB (config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)# lldp enable
SwitchB (Config-If-Ethernet1/0/1)# lldp mode both
SwitchB (Config-If-Ethernet1/0/1)# lldp transmit med tlv capability
SwitchB (Config-If-Ethernet1/0/1)# lldp transmit med tlv network policy
SwitchB (Config-If-Ethernet1/0/1)# lldp transmit med tlv inventory
SwitchB (Config-If-Ethernet1/0/1)# network policy voice tag tagged vid 10 cos 4
```

3) Verify the configuration

```
# Show the global status and interface status on Switch A.
SwitchA# show lldp neighbors interface ethernet 1/0/1
Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :1
PortDesc :****
SysName :****
SysDesc :*****

SysCapSupported :4
SysCapEnabled :4

LLDP MED Information :
MED Codes:
(CAP)Capabilities, (NP) Network Policy
(LI) Location Identification, (PSE)Power Source Entity
(PD) Power Device, (IN) Inventory
MED Capabilities:CAP,NP,PD,IN
MED Device Type: Endpoint Class III
Media Policy Type :Voice
Media Policy :Tagged
Media Policy Vlan id :10
Media Policy Priority :3
Media Policy Dscp :5
Power Type : PD
Power Source :Primary power source
Power Priority :low
Power Value :15.4 (Watts)
Hardware Revision:
```

```
Firmware Revision:4.0.1
Software Revision:6.2.30.0
Serial Number:
Manufacturer Name:****
Model Name:Unknown
Assert ID:Unknown
IEEE 802.3 Information :
 auto-negotiation support: Supported
 auto-negotiation support: Not Enabled
 PMD auto-negotiation advertised capability: 1
 operational MAU type: 1
SwitchA# show lldp neighbors interface ethernet 1/0/2
Port name : interface ethernet 1/0/2
Port Remote Counter：1
Neighbor Index: 1
Port name : Ethernet1/0/2
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :1
PortDesc :Ethernet1/0/1
SysName :****
SysDesc :*****

SysCapSupported :4
SysCapEnabled :4
```

Explanation:

1) Both Ethernet2 of switch A and Ethernet1 of switch B are the ports of network connection device, they will not send LLDP packets with MED TLV information forwardly. Although configure Ethernet1 of switch B to send MED TLV information, it will not send the related MED information, that results the corresponding Remote table without the related MDE information on Ethernet2 of switch A.

2) LLDP-MED device is able to send LLDP packets with MED TLV forwardly, so the corresponding Remote table with LLDP MED information on Ethernet1 of switch A.

11.4 LLDP-MED Troubleshooting

If problems occur when configuring LLDP-MED, please check whether the problem is caused by the following reasons:

☞ Check whether the global LLDP is enabled.

☞ Only network connection device received LLDP packets with LLDP-MED TLV from the near MED device, it sends LLDP-MED TLV. If network connection device configured the command for sending LLDP-MED TLV, the packets also without LLDP-MED TLV sent by the port, that means no MED information is received and the port does not enable the function for sending LLDP-MED information.

☞ If neighbor device has sent LLDP-MED information to network connection device, but there is no LLDP-MED information by checking **show lldp neighbors** command, that means LLDP-MED information sent by neighbor is error.

Chapter 12 PORT SECURITY

12.1 Introduction to PORT SECURITY

Port security is a MAC address-based security mechanism for network access controlling. It is an extension to the existing 802.1x authentication and MAC authentication. It controls the access of unauthorized devices to the network by checking the source MAC address of the received frame and the access to unauthorized devices by checking the destination MAC address of the sent frame. With port security, you can define various port security modes to make that a device learns only legal source MAC addresses, so as to implement corresponding network security management. After port security is enabled, the device detects an illegal frame, it triggers the corresponding port security feature and takes a pre-defined action automatically. This reduces user's maintenance workload and greatly enhances system security.

12.2 PORT SECURITY Configuration Task List

1. Basic configuration for PORT SECURITY

Command	Explanation
Port mode	
switchport port-security **no switchport port-security**	Configure port-security of the interface.
switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>] **no switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>]**	Configure the static security MAC of the interface.
switchport port-security maximum <*value*> [vlan <*vlan-list*>] **no switchport port-security maximum <*value*> [vlan <*vlan-list*>]**	Configure the maximum number of the security MAC address allowed by the interface.
switchport port-security violation {protect | restrict | shutdown} **no switchport port-security violation**	When exceeding the maximum number of the configured MAC addresses, MAC address accessing the interface does not belongs to this interface in MAC address table or a MAC address is configured to several interfaces in same VLAN, both of them will violate the

	security of the MAC address.

switchport port-security aging {static | time <*value*> | type {absolute | inactivity}}
no switchport port-security violation aging {static | time | type}
	Enable port-security aging entry of the interface, specify aging time or aging type.

Admin mode	
clear port-security {all | configured | dynamic | sticky} [[address <*mac-addr*> | interface <*interface-id*>] [vlan <*vlan-id*>]]	Clear the secure MAC entry of the interface.
show port-security [interface <*interface-id*>] [address | vlan]	Show port-security configuration.

12.3 Example of PORT SECURITY

Fig 12-1 Typical topology chart for port security

When the interface enabled Port security function, configure the maximum number of the secure MAC addresses allowed by a interface to be 10, the interface allows 10 users to access the internet at most. If it exceeds the maximum number, the new user cannot access the internet, so that it not only limit the user's number but also access the internet safely. If configuring the maximum number of the secure MAC addresses as 1, only HOST A or HOST B is able to access the internet.

Configuration process:

#Configure the switch.

```
Switch(config)#interface Ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport port-security
Switch(config-if- ethernet1/0/1)#switchport port-security maximum 10
Switch(config-if- ethernet1/0/1)#exit
Switch(config)#
```

12.4 PORT SECURITY Troubleshooting

If problems occur when configuring PORT SECURITY, please check whether the problem is caused by the following reasons:

☞ Check whether PORT SECURITY is enabled normally

☞ Check whether the valid maximum number of MAC addresses is configured

Chapter 13 QSFP+ Port Split and Combination Configuration

13.1 Introduction to QSFP+ Port Split and Combination Configuration

QSFP+ port can be used as a single 40GE port and it also can be splited into 4 10GE SFP+ ports to improve the port density, decrease the user cost and increase flexibility of networks. For example, QSFP+ port of Ethernet1/1/1 is 40GE as default, it can be split into 4 10GE SFP+ ports according to need of Ethernet1/1/1, Ethernet1/1/2, Ethernet1/1/3 and Ethernet1/1/4. The SFP+ ports split support the same configuration and feature as the ordinary SFP+ physical port. QSFP+ port need the dedicated one-to-four wire to connect after split.

If user needs larger bandwidth, the 4 10GE ports can be combined to a 40GE port for using. After combination, the wire should be changed as one-to-one wire. The description of wire is shown in the relevant manual.

QSFP+ port split and combination configuration must be saved and restart the switch, then it will be effective.

13.2 QSFP+ Port Configuration

QSFP+ port configuration task list is as below:

1. Enter global configuration mode
2. QSFP+ port split/combination configuration
3. Configuration retained
4. Restart switch

1. QSFP+ port split/combination configuration

Command	Explanation
Global Mode	
hardware profile module <*module-list*> 4x10G **no hardware profile module <*module-list*> 4x10G**	Split the appointed QSFP+ interface from 40GE port mode into 4 SFP+ 10GE port modes; the no command combines the 4 SFP+ 10GE ports to 1 40GE port.

13.3 Typical Case of QSFP+ Port Configuration

SWITCH configuration task list:

```
Switch >en
Switch #config
Switch (config)#hardware profile module 1 4x10G
The new configuration will take effect after system restart!
Switch (config)#exit
Switch #write
Confirm to overwrite current startup-config configuration [Y/N]:y
Write running-config to current startup-config successful
Switch #%Jun 14 15:34:58 2012 Write configuration successfully!
Switch #reload
```

13.4 QSFP+ Port Configuration Troubleshooting

☞ Configure multiple ports split and combination successively, it will be effective only after configuring and restarting.

☞ For example, for the first QSFP+ port of Module 1, the name in 40G mode is Ethernet1/1/1, after split, it will become 4 10GE QSFP+ ports of Ethernet1/1/1, Ethernet1/1/2, Ethernet1/1/3 and Ethernet1/1/4.

☞ The configuration and feature of each port are the same as the ordinary physical QSFP+ port.

☞ After combination, use the one-to-one wire in 40G mode, both the sides are QSFP+ modules; after split, use the one-to-four wire in 4x10G mode, one side is QSFP+ mode, and the other one is divided into 4 SFP+ modules.

Chapter 14 CFM-OAM Configuration

14.1 Overview

Since the Ethernet technology was naissance, its' simple and low-cost characteristics make it to become the dominant technology in the local area network.Recently, kilomega and million mege apply one after the other, this urges the network providers, facilities manfufaturers and normalizer to advance the Ethernet technology to city and wide network.

Nevertheless, Ethernet is a LAN technology constitutionally. For the need of outlying inspection, SLA (service level protocol) testing are not imminent in the LAN environment, ，therefore the trandition Ethernet does not has the OMA function which is required by the network provider. Other than that, the trandition Ethernet has 10 seconds or the shortest 1 second linkage failure rearrange time is not acceptable by the network providers. Therefore, less than 50 millisecond failure rearrange time is also a big challenge for the city network Ethernet.

After several Ethernet OMA standards (for example, IEEE 802.3ah, IEEE802.1ag and ITU Y.1731) come out, OAM is not the indication weakness of the Ethernet.Using the IEEE802.1agas example, this also go by the name of connection failure management（CFM）standard, it provides the port to port network inspection and operation tools. It can execute the tasks such as MAC Ping, L2 Trace Route etc in the huge L2 Ethernet. It will simplify the failure elimination and SLA inspection in the operation of Ethernet. At the same time, the defined CCM (continuous inspection information) in the OMA standard in Ethernet can actualize undergo the protection rearrange lower than 50 millisecond. The shortest CCM sending time in the standard is 3.3 milliseconds. Three continuous losing CCM message will cause the main link declare invalidation and using the backup link to replace. CFM's effective is built up base on the reasonable dispose of network and configuration.

14.1.1 Ethernet OAM Protocol Criterion

About the Ethernet OAM, there are 4 protocol standard: 802.3ah (the first mile Etherney, short form called EFM), 802.1ag (connection failure management, the short form called CFM), E-LMI (the local port of Ethernrt), Y.1731 (failure and performance inspection), constitute by different group, the corresponding relationship as following:

IEEE 802.3ah：Ethernet Link OAM (EFM OAM)

IEEE 802.1ag：Connectivity Fault Management (CFM)

ITU-Y.1731：OAM functions and mechanisms for Ethernet based network

MEF E-LMI：Ethernet Local Management Interface

EFM OAM and CFM as the constitute to set the IEEE, EFM OAMworking data link layer, as shown in Fig 14-1, can discover and manage the lower layers' data links effectively. Also, we can use EFM OAM technology to increase the management and maintance ability, in order to maintain the stability of operation. CFM is the network level of Ethernet OAM technology, mainly use for the connect pool layer and responds for inspecting the connectedness of the network, orientating the failure of network connectedness. Y.1731 is establish by the ITU, the international telecom union, its' function is mucher bigger than CFM. Can also say that the function which perform by CFM is the subset of Y.1731. E-LMI is established by the MEF; only apply for UNI (the user boundary and the provider boundary that is faced by the user).

14.1.2 CFM OAM Basic Concept

802.1ag divide the whole network (customer, provider, operator) into different MD (Maintenance Domain). In each of the maintance domains, it wills contrapose the MD provided service for maintance management. On these services, there will have a lot of node point facilities. The core idea of the service of 802.1ag is inspecting the involved or all node points, so that it can discover the failure parts. The point that participates in maintance inspection is called MP (Maintenance Point, it is divided into MEP (maintenance edge point) and MIP (maintenance intermediate point)), the bridge of port that configure on the maintance point.

14.1.3 Maintance Domain

The network can be logically divided into different layers from internal to external; it is called MD (Maintenance Domain). The maintenance domain can be nesting but not across. Each of the vindicator can only see it own maintenance domain. The lower level of maintenance can provide the service to the border upon upper layer. Then, it can separate the vindicator e.g. operator and the user clearly. It can orientate the network proble more convenient.

In the network can contains of multi maintenance domain, each of the maintenance domain locates in particular level, totally there are 8 levels. The higher the level, the range of maintenance is higher. The higher level can nesting into lower level of domain. In the reaility, CFM usually applies for the following situation. At this moment, it will divide into customer domain, service provider domain, operator domain etc.

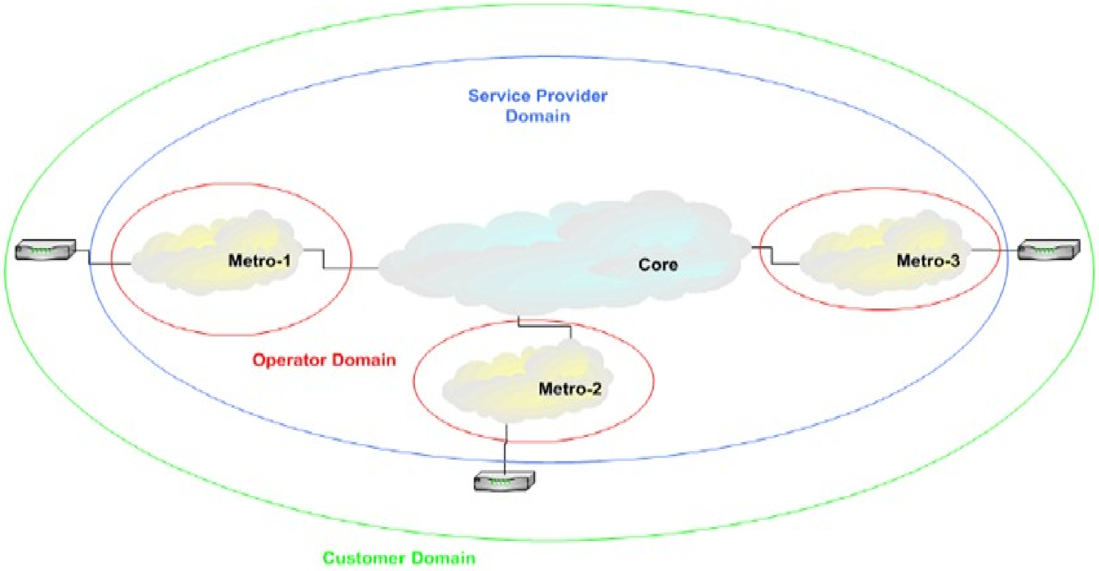

Fig 14-1 Maintenance Domain

Except the level, each of the MD has the global unique MD Name, which uses for lable that MD.

14.1.4 Maintenance Set

Each of the service instances in the maintenance domain is a MA (Maintenance Association). One MD usually provide several service instances externally, 802.1ag is one to one management maintenance and inspect the failure of MA. Each of the MA will have a unique name in the MD. In the network, service instance usually mark by vlanId. And MA is corresponding to the services instances. Therefore, there is a linkage between MA and vlanId. One MA corresponds to one vlanId, at the same time, protocol allows many vlanId manage and maintain by one MA. In these vlanIds, there is a vlan that is a primary vlan. In the MD, there is an uncertainty of one vlanId corresponds to multi MA situation, therefore leave out of account for this moment. All in all, md and primary vlan Id is the unique label of MA.

14.1.5 Maintenance Base Point

It is belong to certain maintenance service, the boundary of the service, which is configured on the port. MEP responds for initiating all CFM messages (CCM,LTM,LBM), the protocol behaviours and the status are mainly occour in the MEP. MEP is divided into UP MEP and DOWN MEP. In the bridge, if MEP is sending and receiving the MA corresponding CFM messages from Lan, then this MEP is Down MEP ; if the MEP is sending and receiving the MA corresponding CFM messages from Bridge Relay, then it is the Up MEP. Shown as following Fig 14-2:

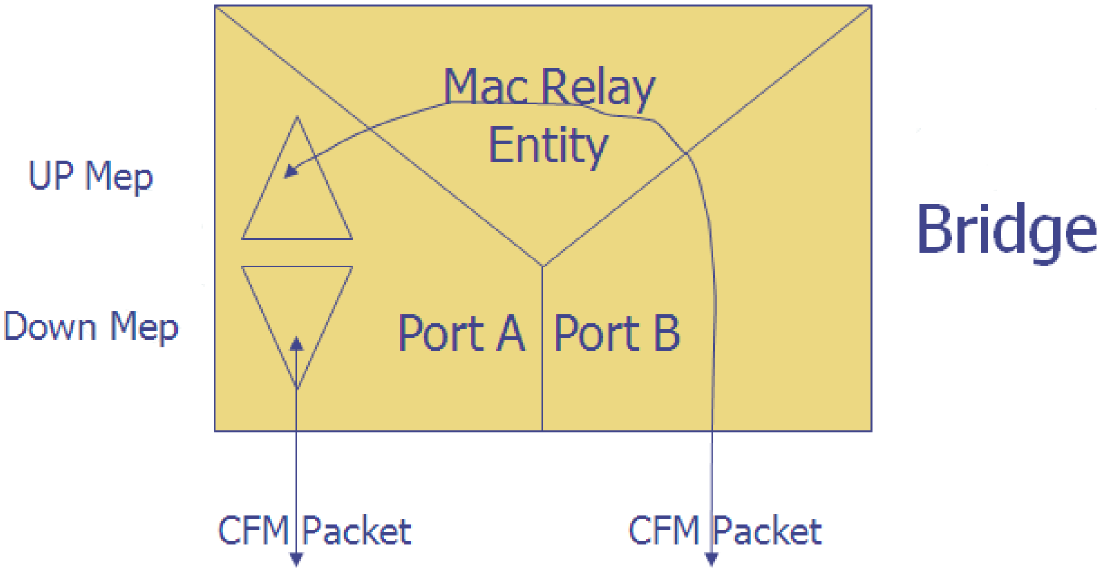

Fig 14-2 The difference between Down MEP and Up MEP

In more esay word, MEP sending and receiving the CFM messages from the local port is the Down MEP; in contrast, it is the Up MEP. MEP inherits the attributes of MD and MA that is located. It means the MD level and vlan Id. Maintenance base point is the only one label in the MA, it can be called MEPID.

14.1.6 Maintenance Mid-Point

It is belongs to certains maintenance service, the mid-point of maintenance service, and configures on the port. MIP cannot send the CFM messages actively; it can only receive the messages from the respond, sending Reply and transmit. It is not in charge of inspection and report failure, but it will assist MEP to undergo the failure inspection. MIP inherits the attributes of MD and MA that is located. It means the MD level and vlan Id.

MIP is not configured directly, it develops according to certain rules of system. In the port, each of the maintenance can only have one MIP. The following is the MIP rules:

none **:** Not build up the MIP node

default **:** If there is not a higher level of MEP on the port, and at the same time, lower level of MIP does not exist, then it will build up MIP on particular port at this level.

explicit **:** If there is not a higher level of MEP on the port, but at the same time, lower level of MEP exists and lower level of MIP does not exist, then it will build up MIP on particular port at this level.

defer **:** Whether build up the MIP node, the build rules will be determine by the configured rules of MD in the MA.

14.2 Introduction of CFM OAM Function

802.1ag provides 5 different functions: Fault detection, Fault verification and isolation, Path discovery, Fault notification and Fault recovery. Thereinto, Fault recovery need to excute with other protocols together.

14.2.1 Inspection of Failure

Maintanence base point （MEP） will send the CCM messages to Remote MEP in the same maintanence collection (MA) periodically. At the same time, it also receives other outlying point CCM message. If it cannot receive the CCM message in 3 months, then it will regards as occour failure in the link and report. The process is shown as follow Fig 14-3 :

CCM messages can also be sent to other MEP in the same MA, it is the group messages. The last 3 bit of the group broadcast address represent different maintanence domain level, thus it can more easy to tackle with hardware.For the lower level of MEP, after it receive higher level of messages, the hardware can accord to group broadcast MAC address and VLAN to undergo the transmitting directly.

The inspection of failure of the periodically sending CCM messages as follow:

- ➢ MEP cannot receive the CCM message on time, represent there is a failure occour in the MA;
- ➢ MEP checking the received CCM messages, it can find out the disagreement failure of the sending time interval;
- ➢ MEP received the failure MEPID or MAID, represent there is exist of internal configuration failure in MA or cross connection failure;
- ➢ MEP receive the lower level of the CCM messages, represent there is exist of internal configuration failure in MA or cross connection failure;
- ➢ MEP receive the CCM message which carries MAC status information, can investigate the outside failure of MA;

Fig 14-3 Connectedness inspection sketch map

14.2.2 Path Discovery

MEP and MIP will through the Linktrace to complete. The function of 802.1ag Linktrace is more or less the same with IP Traceroute. Through send the testing messages and receive replay messages to check the path of destination facilities or orientate the failure point. The processes as follow: MEP send LTM to the target MP（MEP or MIP）, each of the MIP after receiving the LTM will also send a LTR to source MEP. And then, transmit the LTM messages, until the LTM arrive to destination MP or cannot transmit at all. Source MEP according to feedback LTR to confirm the status of the linkage, and obtains the paths to target MAC. It shows in the Fig 14-4 .

LTM destination MAC address is the group broadcast address. The last 3 bit in the group broadcast address represents the level of different maintaence domain. LTR is the one way messages, the destination address as the LTM source MAC address.

Fig 14-4 Path discovery sketch map

14.2.3 Confirmation and Orentation of Failure

It can be actualizing by the 802.1ag Linktrace function that mention above. Also it can be actualizing by 802.1ag Loopback function as well. The circulation function is more or less the same with IP Ping, through out the sending of testing messages and receiving the replay messages to detect whether it can arrive to the destination facility. The idiographic processes as follow: MEP sending the one way broadcast message（LBM）, the destination address of the message is the outlying MP. Once the middle facility receive the LBM will then transmit, and the ouylying MP will sending the replay message (LBR) to the source MEP after it receive the LBM. The source MEP can accord this to determine whether the outlying MP can arrive or not. As shown in the following Fig 14-5.

Fig 14-5 the figure of circulation function

14.2.4 Inform of Failure

After CFM inspects the failure of linkage, there are several of methods to tackle with:

After checking the linkage failure, MEP will send the SNMP TRAP message to the management node, and inform failure occoured;

After checking the linkage failure, MEP will send the records to the facility log book, and the administrators can discover the problem after checking it;

After checking the linkage failure, will cooperate with others automatic protect protocol such as APS etc to undergo recovery. CFM will inform the occourance of failure to these protocols, and confer switching the linkage automatically.

14.3 CFM OAM Basic Function Configuration

14.3.1 The Design of CFM Management Topology

Before the execution of CFM OAM function, need to perform the following layout in the network:

1. Need to divide the levels in the maintenance domain in the whole network, to confirm each level of boundaries in the domain.
2. Confirm the name of each maintenance domain, the name of different facilities is the same in the same maintenance domain.
3. According to the VLAN that is need to inspect, and confirm the maintenance services in different maintenance domains.
4. Confirm each of the name of all maintenance services, the name of different facilities is the same in the same maintenance sercive in the domain.

5. Confirm different facilities are the same in the same maintenance base point table in the same maintanence service of same domain.
6. Can maintance the maintenance base point under the rules of the port in the maintenance domain and boundary of services. And maintance the mid-point in the non- boundary or port.

Therefore require for the following data:

Serial number	Data
1	MD name and level
2	MA name, MA related VLAN ID
3	MEP ID, the name of the port that is connected to MEP, types of MEP
4	RMEP ID
5	MIP develop rules
6	The time interval that sending and detecting CCM news from MEP in MA

14.3.2 CFM OAM Configuration Task List

1. Select to enable CFM OAM function mode
2. Enable CFM OAM function globally
3. Enable y1731 function globally (selectable)
4. Create MD
5. Create MA
6. Create MEP
7. Configure RMEP
8. Create MIP (selectable)
9. Enable the failure confirmation function (selectable)
10. Configure CC sending and detecting
11. Check the configuration result of CFM

1. Select to enable CFM OAM function mode

Command	Explanation
Global Mode	
ethernet cfm mode {hw|sw|auto} **no ethernet cfm mode**	Select the mode of enabling CFM OAM; it is only used before enabling CFM OAM function. No command recovers to be the default of auto.

2. Enable CFM OAM function globally

Command	Explanation
Global Mode	

ethernet cfm global **no ethernet cfm global**	Enable CFM OAM function globally. No command disables this function.

3. Enable y1731 function globally (selectable)

Command	Explanation
Global Mode	
ethernet cfm y1731 global **no ethernet cfm y1731 global**	Open the Y1731 function. After initial this function, the switch will ente into the y1731 mode. The messages are sending and decoding in the Y1731 format. **Notice:** It need to use the ethernet cfm global command before using this command, otherwise, it cannot be function. No command disables it.

4. Create MD

Command	Explanation
Global Mode	
ethernet cfm domain < *domain-name* > level < *level-id* > ***no* ethernet cfm domain < *domain-name* >**	Build up MD , enter into the MD configuration mode. If the MD is created successfully, thelevel will not be allowed to modify. No command deletes the created MD.
MD Configuration Mode	
id {mac-address XX-XX-XX-XX-XX-XX domain-number < *domain-number* > | dns < *dns-name* > | null } **no id**	Configure MDID. Domain-name which is configured by the name of maintance domain will use the command of ***ethernet cfm domain*** will not be fill in the message. Fill in the MDID and ma name will create MAID; the total length of MAID is 44. The length cannot be existed; otherwise, it will have error. No command deletes the configured id.

5. Create MA

Command	Explanation
MD Configuration Mode	

service { < *ma-name* > | number < *ma-num* > | pvlan < *vlan-id* > }{ port | pvlan < *vlan-id* > } [vlan < *WORD* >] [direction down] **no service { < ma-name > | number < ma-num > | pvlan < vlan-id > }**	Build up MA. Configure the property of UP/DOWN of MA and enter into MA mode. One service can related to one or more vlan. If MA is created successfully, the association vlan and UP/DOWN property will not be allowed to modify. If there is need to modify, delete the MA first and create it again.One switch can configure maximum 512 MA. No command deletes the created MA.

6. Create MEP

Command	Explanation
MA Configuration Mode	
mep mepid < *WORD* > **no mep mepid [< *WORD* >]**	Using this command to build up the permit configured MEP table in the maintance collection. No command deletes the created MEP.
Port Mode	
ethernet cfm mep < *mepid* > domain < *domain-name* > service { < *ma-name* > | number < *ma-num* > | pvlan < *vlan-id* > } **no ethernet cfm mep < mepid > domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > }**	Build up MEP on port. The MEP property has been formed when creating the MA. If MA is UP/DOWN property, all MEP points in this MA are UP-DOWN property. No command deletes the created MEP.

7. Configure RMEP

Command	Explanation
MA Configuration Mode	
continuity-check receive rmep <*mep-id*> [active time < *time* >] **no continuity-check receive rmep <*mep-id*>**	Open CCM message receiving function and build up rmep in MA. If the mepid in an MA has been configured as MEP, it cannot be configured as RMEP. No command deletes the configured RMEP.

8. Create MIP (selectable)

Command	Explanation
MD Configuration Mode; MA Configuration Mode	

mip auto-create [lower-mep-only | none] **no mip auto-create**	Configure the automatic MIP in the maintance collection's domain. As default, there is no rule of configuring the mid point; and it does not carry the sender-id. No command deletes the MIP.
Global Mode	
ethernet cfm mip auto-create level < ***level-id*** **> vlan <** ***WORD*** **> [lower-mep-only] [sender-id chassis]** **no mip auto-create**	Build up the MIP configureation on the layer that does not relate to MA. As default, there is no rule of configuring the mid point; and it does not carry the sender-id. No command deletes the MIP.

9. Enable the failure confirmation function (selectable)

Command	Explanation
Global Mode	
ethernet cfm alarm {delay < ***mseconds*** **> | notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon} | reset <** ***mseconds*** **>}** **no ethernet cfm alarm { delay | notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon} | reset }**	Enable the function of error alarm. No command recovers to be default.
ethernet cfm logging **no ethernet cfm logging**	Open the log record function. If alarm is occour, it means that has already recorded or inform out of order. No command disables this function.
ethernet cfm snmp-server enable traps **no ethernet cfm snmp-server enable traps**	Having the snmp notification during the alarm. If the set up is success, it will have the snmp notification during the alarm. No command disables this function.

10. Configure CC sending and detecting

Command	Explanation
MA Configuration Mode	
continuity-check enable **no continuity-check enable**	Using this command to open the maintance point of CCM message sending and receiving functions. No command cancels the local CCM packets sending and detection.

continuity-check interval < *interval-value* > **no continuity-check interval**	Configure the time interval value for sending message from MEP to CCM. Under the software mode, the minimum sending cycle is 100ms (interval value=3) and under the hardware mode, the minimum sending cycle is 3.3ms (interval value=1). No command recovers to be 1s (interval value=4).

11. Check the configuration result of CFM

Command	Explanation
Admin Mode	
show ethernet cfm domain { < domain_name > | brief }	Display the configured information of maintance domain.
show ethernet cfm service [domain < *domain-name* > [service { ma-name | number < *ma-num* > | pvlan < *vlan-id* > }]]	Display the configured information of the maintance collection.
show ethernet cfm maintenance-points local [detail] [mep | mip] [domain < *domain-name* > | interface { ethernet | } <*IFNAME*>]	Display the attribute and the operation information of the maintance basepoint.
show ethernet cfm maintenance-points remote detail (mac XX-XX-XX-XX-XX-XX | domain WORD (service ((WORD)|(number <*0-65535*>)|(pvlan <*1-4094*>))) mepid <*1-4094*>)	Display the attribute and the operation information for the outlaying maintance base point.
show ethernet cfm maintenance-points remote (domain WORD (service (WORD|number <*0-65535*>| pvlan <*1-4094*>) (mepid <*1-4094*>|)|)|)	Display the attribute and operation information of outlaying maintance base point.
show ethernet cfm statistic [domain < *domain-name* > [service { ma-name | number < *ma-num* > | pvlan < *vlan-id* > }]]	Display the message sending statistics information in the CFM of the facility.

14.4 CFM OAM Failure Confirmation

14.4.1 The Confirmation of Management topology

Before excute the failure confirmation, please ensure to finish the configuration of CFM OAM function.

The following data are needed to the inspection of failure manually:

Serial number	Data
1	MD name
2	MA name
3	Destination MEP ID or MAC
4	The require number, size and overtime of sending message from the loopback function.
5	The TTL value of linktrace functionwhich need to send

14.4.2 Implement Loopback Function

Under the admin mode, implement the commands:

Command	Explanation
Admin Mode	
ping ethernet [target-mep < ***mepid*** **> | target-mac <** ***mac-address*** **>] {domain <** ***domain-name*** **> service { <** ***ma-name*** **> | number <** ***ma-num*** **> | pvlan <** ***vlan-id*** **> }} [number <** ***number*** **>] [packetsize <** ***size*** **>] [timeout <** ***timeout*** **>]**	Open the circulate function. Send LBM messages and receiving LBR message from a particular maintance point to the other points. Under the default stage, this function is closed. If enter into target-mep-id, it cannot searching the corresponding mac address. If it cannot find, it will display error. If you enter the mac address, then will according to this address for the circulation. If it is a domain-name, then it require opening the y1731function, then sending the group broadcast LBM message.

14.5 CFM OAM Failure Orientation

14.5.1 Management topology Confirmation

Before excute the confirmation of failure, please ensure the completion of CFM OAM function configuration.

To testing the failure manually need to prepare the following data:

Serial number	Data
1	MD name
2	MA name
3	Destation MEP ID or MAC
4 (selectable)	The largest run after reading
5 (selectable)	Only enquire for FDB; or need to enquire both FDB and MIP data for undergo the failure confirmation

6 (selectable)	MEP ID that initiates LTM

14.5.2 CFM OAM Failure Orientation Task List

1. **Implement linktrace function**

Command	Explanation
Admin Mode	
traceroute ethernet { target-mep < ***target-mep-id*** **> | target-mac <** ***mac-address*** **> } {domain <** ***domain-name*** **> service { <** ***ma-name*** **> | number <** ***ma-num*** **> | pvlan <** ***vlan-id*** **> }} [fdb-only | source <** ***mepid*** **>]] [ttl <** ***ttl-value*** **>]**	Check the path from the appointed maintaining point to the target point. As default, ttl=64 and inquiry FDB and MIP database.

2. **Configure auto-linktrace function (selectable)**

Command	Explanation
MA Configuration Mode	
traceroute ethernet auto **no traceroute ethernet auto**	Enable the function of sending the link track packets automatically. Enable the function of sending the link track packets automatically. As default, this function is disabled. **Notice:** After enabled this function, when the maintaining point does not receive the CCM packets from the distant point in 3.5 sending cycles of CCM packets, judge that the connection to the distant point is wrong, then send LTM packet (the target of this LTM packet is the distant maintaining point, the TTL field in LTM packet is the maximum value of 255) to locate the error through detecting the responsed LTR packet. No command disables this function.
Global Mode	
ethernet cfm auto-traceroute cache { size < ***size-value*** **> | hold-time <*minutes*>}** **no ethernet cfm auto-traceroute cache { size | hold-time }**	Configure saving the size of automatic LT detection result or over time result. As default, The buffer just records the 5 least automatic detection result, the overtime as 100minutes. No command recovers to be default.

3. **View the result of auto-linktrace**

Command	Explanation
Admin Mode	
show ethernet cfm traceroute-reply auto [domain < *domain_name* > [service { ma-name | number < *ma-num* > | pvlan < *vlan-id* > }]]	Display the result of the automatic LT. If there is no appointed domain, then it will display all the automatic LT result in the facilities. If there is no appointed ma, then it will display particular domain's automatic LT result in the facilities.

14.6 ULPP Linkage (Selectable)

14.6.1 ULPP Linkage Task List

1. Configure ulpp linkage

☞ Configure with the topology and ensure CC function is running normally.

☞ Configure the ULPP function first.

☞ ULPP linkage is just with down MEP.

☞ The vlan associated with linkage MEP must be in the protection vlan of the relevant ULPP group.

Command	Explanation
Port Mode	
switchport ulpp group <*group-id*> track cfm cc level <*level-value*>	Configure ulpp group member port to associate with cfm cc detection. When ulpp group member port received the matching cfm information (timeout or recover), conduct the association.

2. Check the result of ULPP linkage configuration

Command	Explanation
Admin Mode	
show ulpp group <*word*>	Check the result of ULPP association configuration. If the configuration is successful, the level of MD in Track-cfm-level will be shown.

14.6.2 Example of ULPP linkage application

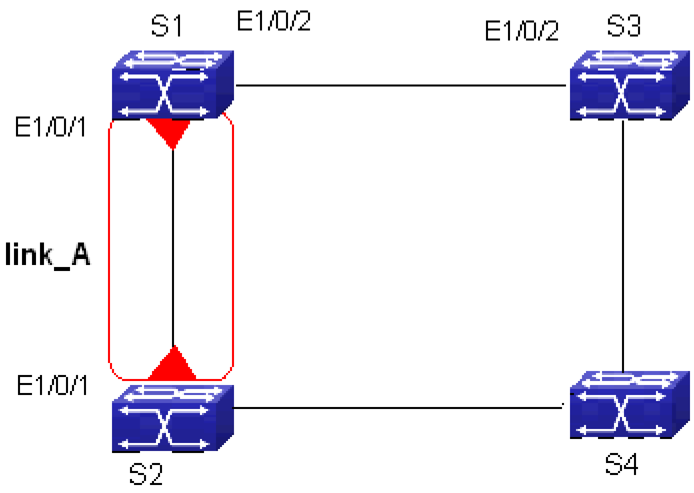

Fig 14-6 ULPP linkage application Figure

1. **The consider path of configuration:**

Using the following path of configuration to configure the ULPP linkage function:
Build up the VLAN, and adding the related ports to corresponding VLAN.
Build up the MD link_A in S1, S2 and the level is 4
Build up and configure MA1 in customer_A（MA1 and VLAN1 related）
Configure corresponding MEP and RMEP in the S1 and S2
Build up the ulpp group1 in S1 and configure the main and assist port
Configure corresponding flush receiving port to S2 and S3
Configure linkage port in the S1

2. **Steps of Configuration**

(1) Build up VLAN, and adding the related ports to corresponding VLAN

(2) Build up the MD link_A and corresponding MEP and RMEP in S1 and S2

```
# Build up the link_A in S1 and configure corresponding MEP and RMEP
Switch(config)#ethernet  cfm domain link_A level 4
Switch(config-ecfm)#service MA1 pvlan 1 direction down
Switch(config-ecfm-srv)#mep mepid 1-2
Switch(config-ecfm-srv)#continuity-check enable
Switch(config-ecfm-srv)#continuity-check receive rmep 2
Switch(config-ecfm-srv)#exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#ethernet cfm mep 1 domain link_A service MA1
```

Using the same method to build up the link_A in S2 and configure corresponding MEP and RMEP

(3) Build up the ulpp group 1 in S1 and protect vlan1

```
# Build up the ulpp group 1 in S1 and open the grabbing mode to protect vlan
Switch(config)#spanning-tree mst configuration
Switch(config-mstp-region)#instance 1 vlan 1
Switch(config-mstp-region)#exit
Switch(config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#flush enable mac-vlan
Switch(ulpp-group-1)#preemption mode
# configure the 1/0/1 in S1 to become the master port, and the 1/0/2 as slave port
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#ulpp group 1 master
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#ulpp group 1 master
# Configure the receiving port 1/0/1 in S2 to receive flush message
Switch(config-if-ethernet1/0/1)#ulpp flush enable mac-vlan
```

Using the same method to onfigure the receiving port 1/0/2 in S3 to receive flush message

(4) Configure ulpp linkage in the S1

```
# Configure ulpp linkage in the 1/0/1 port in S1
Switch(config-if-ethernet1/0/1)#switchport ulpp group 1 track cfm level 4
```

3. **Checking the configuration result**

```
# Checking the ulpp linkage configuration result in S1
Switch(config)#show ulpp group 1
ULPP group 1 information:
Description:
Preemption mode: ON
Preemption delay: 30s
Control VLAN: 1
Flush packet: MAC MAC-VLAN  ARP
Protected VLAN: Reference Instance 1
Member          Role        State        Track-cfm-level
------------------------------------------------------------------------------------
Ethernet1/0/1    MASTER     FORWARD          4
Ethernet1/0/2    SLAVE       STANDBY           -
------------------------------------------------------------------------------------
```

# if the CFMchecking the CC is overtime, then it will inform the ULPP function to undergo the switching of main and assist ports:

```
%Jan 01 00:12:19 2012 ULPP: ULPP group 1:Master port Ethernet1/0/3 receives cfm event type:CFM_ALARM_RMEP_CCM vlan:1 level:4.
%Jan 01 00:12:19 2006 ULPP: ULPP group 1:Master port Ethernet1/0/3 change state to down,Slave port Ethernet1/0/1 change state to forwarding.
%Jan 01 00:12:21 2006 CFM:A CFM_ALARM_RMEP_CCM of Interface Ethernet1/0/3 is detected.
```

14.7 Example of Configuration Application

The following Fig 14-7 is the CFM configuration application illustration, in order to actualize the inspection of the status of linkage, can follow the steps as shown below to undergo the configuration.

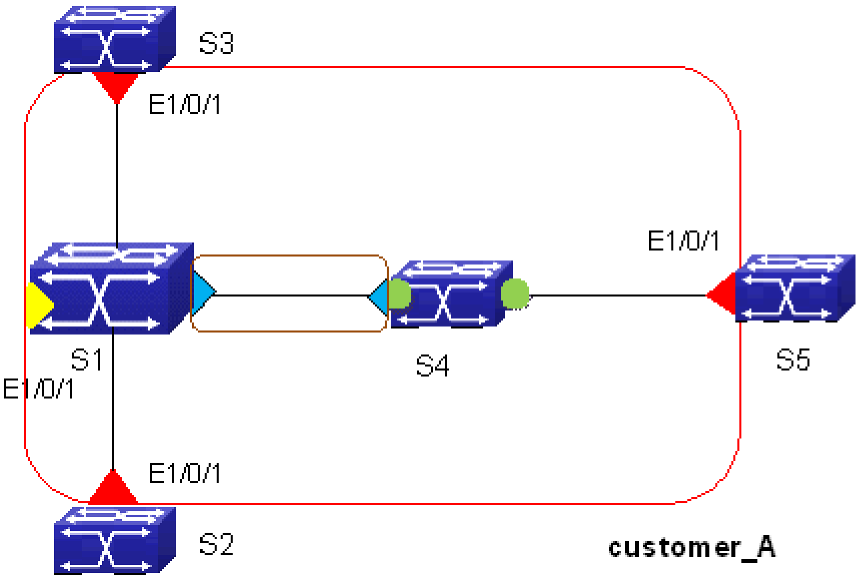

Fig 14-7 MD, MA, MEP and MIP configuration figure

1. **The consider path of configuration**

Using the following path of configuration to configure the Ethernet CFM basic function:

Build up the VLAN, and adding the related ports to corresponding VLAN.

Build up the customer_A on the facilities S1、S2、S3、S4、S5 , the level of customer_A is 6.

Build up and configure MA1 in customer_A（MA1 and VLAN1 related）

Build up operator_A in the facilities S1, S5, the level of operator_A is 3

Build up and configure MA2 in operator_A（MA2 and VLAN2 related）

Build up local and outlying MEP in the MA1 of customer_A in the S1, S2, S3, and S4

Build up MIP in the customer_A of S4

Configure local and outlying MEP in the MA2 of customer_A in the 在 S1,S5

Initial the sending and receiving function of CCM information

2. **Steps of Configuration**

(1) Build up VLAN, and adding the related ports to corresponding VLAN

(2) Open the Global CFM function and build up customer_A and configure MA1

```
# Build up the customer_A in S1, and configure the UP direction MA1
Switch(config)#ethernet cfm global
Switch(config)#ethernet cfm domain customer_A level 6
Switch(config-ecfm)#service MA1 pvlan 1
```

(3) Build up the customer_A and configure the MA1 on the S2, S3, S4, and S5

# Build up the customer_A in S2, and configure the Down direction MA2

```
Switch(config)#ethernet cfm global
Switch(config)#ethernet cfm domain customer_A level 6
Switch(config-ecfm)#service MA1 pvlan 1 direction down
```

Using the same method to build up the MD and MA on other facilities

(4) Build up local and outlying MEP in the MA1 of customer_A in the S1, S2, S3, and S4, also build up the MIP in S5.

#Build up MEP list as 1-4 in the MA1 of S1, configure RMEP2-4, and build up the Etherne1/0/1 on MEP1.

```
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 2-4
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#ethernet cfm mep 1 domain customer_A service MA1
```

# Build up MEP list as 1-4 in the MA1 of S2, configure RMEP1; 3-4, and build up the Etherne1/0/1 on MEP2.

```
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 1；3-4
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#ethernet cfm mep 2 domain customer_A service MA1
```

# Build up MEP list as 1-4 in the MA1 of S3, configure RMEP1; 2; 4, and build up the Etherne1/0/1 on MEP3.

```
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 1；2；4
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#ethernet cfm mep 3 domain customer_A service MA1
```

# Build up MEP list as 1-4 in the MA1 of S4, configure RMEP1-3, and build up the Etherne1/0/1 on MEP3.

```
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 1-3
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#ethernet cfm mep 4 domain customer_A service MA1
```

Using the defaultrules to build up MIP in the MA1 on S5

```
Switch(config-ecfm-srv)#mip auto-create
```

(5) Build up operator_A and configure MA2 on S1 and S5

#Build up operator_A on S1and configure MA2, the types as port

```
Switch(config)#ethernet cfm domain operator_A  level 3
Switch(config-ecfm)#service MA2 port direction down
```

Using the same method (S5) mention above to build up operator_A and MA2

(6) Build up local and outlying MEP in the MA2 of operator_A in the S1 and S5

# Build up MEP list as 1-2 in the S1, configure RMEP2, and build up the Etherne1/0/2 on MEP1.

```
Switch(config-ecfm-srv)#mep mepid 1-2
Switch(config-ecfm-srv)#continuity-check receive rmep 2
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/1)#ethernet cfm mep 1 domain customer_A service MA2
```

# Build up MEP list as 1-2 in the S2, configure RMEP1, and build up the Etherne1/0/2 on MEP2.

```
Switch(config-ecfm-srv)#mep mepid 1-2
Switch(config-ecfm-srv)#continuity-check receive rmep 1
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/1)#ethernet cfm mep 2 domain customer_A service MA2
```

(7) Initial the sending and receiving function of CCM information in S1, S2, S3, S4 in MA1

# Initial the sending and receiving function of CCM information in S1in MA1

```
Switch(config-ecfm-srv)#continuity-check receive enable
```

Other facilities using the same method to initial the CC function.

# Initial the sending and receiving function of CCM information in S1 and S5 in MA

```
Switch(config-ecfm-srv)#continuity-check receive enable
```

(8) To check the configuration of maintanence base point of MA1 in customer_A of S1

```
Switch#show ethernet cfm maintenance-points local detail mep domain customer_A
Mepid:1
Port:Ethernet1/0/1                  Active:1
Domain Name: customer_A
Service Name:MA1
Level:6
Vlan:1                              Direction:Up
-----------------------------------------------------------------------------------------------------
```

```
      CCM:
      CC Send:Enable
CC Received:Enable                  Interval:1(s)
```

14.8 CFM Troubleshooting

Undergo the configuration, using the CFM-OAM, it will occour errors and do not operate normally due to physical connection, configuration error.

☞ Ensure the whole link connection is normal, and the MA needed related vlan is existed.

1. **Configuration Failure**

☞ Ensure the system open the global OAM function, otherwise, it will failure to configure any related OAM commands

☞ Illegal configured MA/MD name：

MD name： 1 ~ 43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline.

MA name：1 ~ 43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline. The sum of MA and the domain name cannot excess than 44 characters.

☞ In the same level, a primary vlan can only be related by one MA.

☞ MD level, MA related pvlan and UP/DOWN attribute cannot be changed after develop

☞ Need to build up the MEP ID before configure the MEP and RMEP

☞ MEP ID in one MA , after configured as MEP, the nit cannot be change to configure RMEP

☞ The DOWN attribute of MA in one facility can only allow existing one MEP; one UP attribute MA can allow to exist of several of MEP, but it cannot allow to configure several identical MA MEP to the same port.

2. **Cannot build up the CC connection**

☞ Through the ***show ethernet cfm*** to checking, ensure both ports' level, MD name, MA name, MA related pvlan are the same.

☞ Ensure the configuration of RMEP of this port is same with the configured MEP ID at the other port.

☞ Ensure this port and the other port opened the CC sending and checking function

☞ Ensure the CCM sending period is the same for two port

☞ Configured the down mep on the port, then mep will receive the message from this port. If it configured the up mep, then the mep will receive the messages from others ports. Please ensure that the up mep configuration is on the non-receiving port.

☞ The port that is blocking by STP protocol cannot receiving, sending, replying the CFM messages. If it is configured as MEP, then even if that port was blocked by the STP protocol, it can still sending and receiving CCM messages. Only the second layer Ethernet port can support the CFM function.

☞ MEP and MIP can configure on the port channel, but at the same time, port channel configured MEP and MIP will ineffective on the members. If you want to increase the CFM MEP and MIP port to port channel, then that port's MEP and MIP will ineffective as well. If you want to recover the MEP and MIP on the port, then need to delete the port-channel from this port.

3. Cannot create the MIP point

☞ Ensure the develop rules of MIP is correct

Default rules：If there is not a higher level of MEP on the port, and at the same time, lower level of MIP does not exist, then it will build up MIP on particular port at this level.

Explicit rules：If there is not a higher level of MEP on the port, but at the same time, lower level of maintanence mid-point does not exist, then it will build up the mid-point depends on whether there is a maintanence base point on lower level.

☞ It will only develop the MIP as the port status as UP; one port bases on one vlan to develop only one MIP; lower MIP point will have higher priority to develop.

☞ A DOWN attribute MA is only need to configureon the port, if there is configured the MEP point in the port, then it cannot develop the MIP, even if there is configured the port-channel, it will cause the MEP ineffective. MIP cannot develop in the MA.

If it cannot slove the proble of CFM OAM after checking, then please using the ***debug ethernet cfm*** etc command, and copy the DEBUG information (3 minutes), and then sending to the technical center of our company.