

目录

第 1 章 端口配置	1-1
1.1 端口介绍	1-1
1.2 业务端口配置	1-1
1.3 端口配置举例	1-3
1.4 端口排错帮助	1-4
第 2 章 端口隔离功能操作配置	2-1
2.1 端口隔离功能简介	2-1
2.2 端口隔离功能任务序列	2-1
2.3 端口隔离功能典型案例	2-2
第 3 章 端口环路检测功能操作配置	3-1
3.1 端口环路检测功能简介	3-1
3.2 端口环路检测功能配置任务序列	3-1
3.3 端口环路检测典型案例	3-3
3.4 端口环路检测排错帮助	3-3
第 4 章 ULDP 操作配置	4-1
4.1 ULDP 功能简介	4-1
4.2 ULDP 配置任务序列	4-2
4.3 ULDP 功能典型案例	4-4
4.4 ULDP 排错帮助	4-5
第 5 章 LLDP 功能操作配置	5-1
5.1 LLDP 功能简介	5-1
5.2 LLDP 功能配置任务序列	5-1
5.3 LLDP 功能典型案例	5-4
5.4 LLDP 功能排错帮助	5-4
第 6 章 Port Channel 配置	6-1

6.1 Port Channel 介绍	6-1
6.2 LACP 简介	6-2
6.2.1 静态 LACP 汇聚	6-2
6.2.2 动态 LACP 汇聚	6-2
6.3 Port Channel 配置任务序列	6-3
6.4 Port Channel 举例	6-4
6.5 Port Channel 排错帮助	6-7
第 7 章 MTU 配置	7-1
7.1 MTU 介绍	7-1
7.2 MTU 配置任务序列	7-1
第 8 章 EFM OAM 配置	8-1
8.1 EFM OAM 介绍	8-1
8.2 EFM OAM 基本配置	8-3
8.3 EFM OAM 举例	8-5
8.4 EFM OAM 排错帮助	8-6
第 9 章 bpdu-tunnel 配置	9-1
9.1 bpdu-tunnel 介绍	9-1
9.1.1 bpdu-tunnel 的作用	9-1
9.1.2 bpdu-tunnel 的产生背景	9-1
9.2 bpdu-tunnel 配置任务序列	9-1
9.3 bpdu-tunnel 举例	9-2
9.4 bpdu-tunnel 排错帮助	9-3
第 10 章 LLDP-MED	10-1
10.1 LLDP-MED 介绍	10-1
10.2 LLDP-MED 配置任务序列	10-1
10.3 LLDP-MED 举例	10-3
10.4 LLDP-MED 排错帮助	10-6
第 11 章 PORT SECURITY	11-1
11.1 PORT SECURITY 介绍	11-1

11.2 PORT SECURITY 配置任务序列	11-1
11.3 PORT SECURITY 举例.....	11-2
11.4 PORT SECURITY 排错帮助.....	11-2
第 12 章 DDM 配置	12-1
12.1 DDM 介绍	12-1
12.1.1 DDM 简介	12-1
12.1.2 DDM 功能.....	12-2
12.2 DDM 配置任务序列.....	12-2
12.3 DDM 举例	12-4
12.4 DDM 排错帮助	12-7

第1章 端口配置

1.1 端口介绍

交换机端口包括电口和 Combo 端口， Combo 端口可以选择配置为千兆电口，也可以选择配置为千兆 SFP 光口，两者只能选择其中之一。

如果用户要对某些端口进行配置，可以使用命令 `interface ethernet <interface-list>` 进入到相应的以太网接口配置模式，参数<interface-list>为一个或多个端口，<interface-list>包含多个端口时，可以使用‘;’和‘-’等特殊字符进行连接，‘;’连接不连续的端口号，‘-’连接连续的端口号。例如要同时对前面板上的 2,3,4,5 端口进行操作，可以使用命令 `interface ethernet 1/0/2-5`。在以太网接口配置模式下可对端口的速率、双工模式、流量控制等进行配置，相应物理端口的表现也随之改变。

1.2 业务端口配置

- 业务端口配置任务序列如下：
- 1. 进入业务端口配置模式
 - 2. 配置业务端口的属性
 - (1) 配置组合端口的组合模式
 - (2) 打开或关闭端口
 - (3) 配置端口名字
 - (4) 配置端口连线类型
 - (5) 配置端口速率和双工模式
 - (6) 配置带宽控制
 - (7) 配置流量控制
 - (8) 打开或关闭端口环回功能
 - (9) 配置交换机广播风暴抑制功能
 - (10) 配置扫描端口方式
 - (11) 配置端口速率违背控制
 - (12) 配置端口速率设置统计间隔时间
 - (13) 设置端口不接收报文
 - 3. 虚拟线路检测

1.进入以太网端口配置模式

命令	解释
全局配置模式	
interface ethernet <interface-list>	进入业务端口配置模式。

2.配置以太网端口属性

命令	解释
端口配置模式	
media-type {copper copper-preferred-auto fiber sfp-preferred-auto}	设定组合端口模式（仅限组合端口）。
shutdown no shutdown	关闭或打开指定端口。
description <string> no description	设定或取消指定端口的名字。
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	设置 1000Base-TX、100Base-TX 或 100Base-FX 端口的速率和双工模式。本命令的 no 操作为恢复默认设置，即自动协商速度双工。
negotiation {on off}	打开或关闭 1000Base-FX 端口的自动协商。
bandwidth control <bandwidth> [both receive transmit] no bandwidth control	设置或取消指定端口收、发数据占用的带宽。
flow control no flow control	打开或关闭指定端口的流量控制功能。
loopback no loopback	打开或关闭指定端口的环回测试功能。
storm-control {unicast broadcast multicast} <packets>	打开交换机的广播风暴抑制（或组播、未知单播，下同）功能，并设置每秒允许通过的广播包数量；本命令的 no 操作为取消广播风暴抑制功能。
port-scan-mode {interrupt poll} no port-scan-mode	配置扫描端口方式为中断或查询方式。本命令的 no 操作恢复默认的端口扫描方式。
rate-violation <200-2000000> [recovery <0-86400>] no rate-violation	设置交换机端口的报文最大收包速率，如果端口的接收报文速率违背了收包速率则 shutdown 端口，可以配置 shutdown 端口后的恢复时间，默认是 300s。本命令的 no 操作为关闭端口的速率违背功能。
switchport discard packet { tag untag } no switchport discard packet { tag untag }	设置端口不接收 tag 报文或 untag 的报文；本命令的 no 操作取消端口的 discard 限制，即允许端口接收 tag 报文或 untag 的报文。

全局配置模式	
port-rate-statistics interval <interval -value>	配置 port-rate-statistics 统计间隔时间。

3. 虚拟线路检测

命令	解释
特权模式	
virtual-cable-test interface (ethernet)IFNAME	进行端口的虚拟线路检测。

1.3 端口配置举例

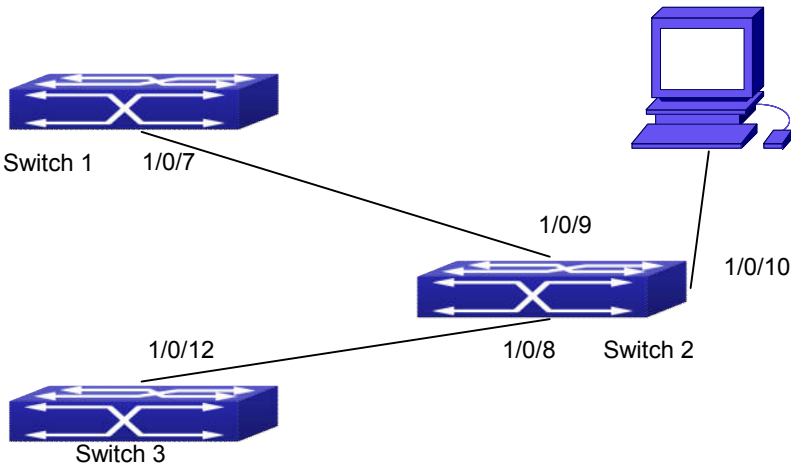


图 1-1 端口配置举例

交换机中均未配置 VLAN，因此使用缺省 VLAN1。

交换机	端口	属性
SW1	1/0/7	入口带宽限制，50M
SW2	1/0/8	端口镜像源端口
	1/0/9	100M/full、端口镜像源端口
	1/0/10	1000M/full、端口镜像目的端口
SW3	1/0/12	100M/full

配置如下：

SW1：

Switch1(config)#interface ethernet 1/0/7

Switch1(Config-If-Ethernet1/0/7)#bandwidth control 5000 both

SW2：

Switch2(config)#interface ethernet 1/0/9

Switch2(Config-If-Ethernet1/0/9)#speed-duplex force100-full

Switch2(Config-If-Ethernet1/0/9)#exit

Switch2(config)#interface ethernet 1/0/10

```
Switch2(Config-If-Ethernet1/0/10)#speed-duplex force1g-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
SW3:
Switch3(config)#interface ethernet 1/0/12
Switch3(Config-If-Ethernet1/0/12)#speed-duplex force100-full
Switch3(Config-If-Ethernet1/0/12)#exit
```

1.4 端口排错帮助

用户在进行端口配置时通常会遇到的情况及解决建议如下：

- ☞ 两个光口互相连接时，如果一端设置为自动协商，另一端设置强制速率/双工，则光口不会 Link up。这是由 IEEE 802.3 协议决定的。
- ☞ 建议用户不要进行以下的组合设置：打开某端口流控，同时设置该端口组播抑制；设置某端口的广播、组播或未知单播抑制，同时设置端口带宽限制。如果在端口进行这些组合设置，可能导致端口流量低于期望值。
- ☞ 对于 Combo 端口，支持强制电和强制光模式，默认为强制光模式，此时插电缆端口不会 UP。

第2章 端口隔离功能操作配置

2.1 端口隔离功能简介

端口隔离是一个基于端口的独立功能，作用于端口和端口之间，隔离相互之间的流量，利用端口隔离的特性，可以实现 **vlan** 内部的端口隔离，从而节省 **vlan** 资源，增加网络的安全性。配置端口隔离功能后，一个隔离组内的端口之间相互隔离，不同隔离组的端口之间或者不属于任何隔离组的端口与其他端口之间都能进行正常的数据转发。一台交换机上最多能够配置 16 个隔离组。

2.2 端口隔离功能任务序列

1. 创建隔离组
2. 将以太网端口添加进隔离组
3. 指定需要隔离的流量
4. 显示端口隔离的配置情况

1. 创建隔离组

命令	解释
全局配置模式	
isolate-port group <WORD> no isolate-port group <WORD>	设置隔离组；本命令的 no 操作将删除隔离组。

2. 将以太网端口添加进隔离组

命令	解释
全局配置模式	
isolate-port group <WORD> switchport interface [ethernet port-channel] <IFNAME> no isolate-port group <WORD> switchport interface [ethernet port-channel] <IFNAME>	将一个或一组以太网端口加入某个隔离组成为该隔离组的隔离端口；该命令的 no 操作是将一个或一组以太网端口从某个隔离组中移出。

3. 指定需要隔离的流量

命令	解释
全局配置模式	
isolate-port apply [<I2 I3 all>]	使端口隔离的配置应用于隔离 2 层流量、隔离 3 层流量或者隔离所有的流量。

4. 显示端口隔离的配置情况

命令	解释
特权配置模式和全局配置模式	
show isolate-port group [<WORD>]	显示端口隔离的相关配置，包括已经配置的隔离组和隔离组内的所有以太网端口。

2.3 端口隔离功能典型案例

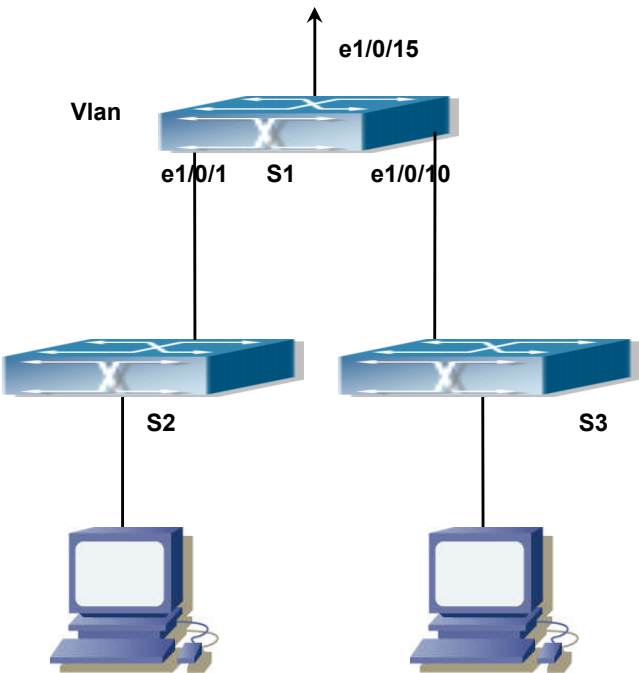


图 2-1：端口隔离功能配置案例

各个交换机的拓扑和配置如上图所示，e1/0/1、e1/0/10 和 e1/0/15 都属于 vlan 100。要求在交换机 S1 上配置端口隔离后，交换机 1 的 e1/0/1 和 e1/0/10 不通，但 e1/0/1 和 e1/0/10 可以和上行口 e1/0/15 通。即，所有下行端口之间不能互通，但下行端口可以和指定的上行端口互通。上行端口可以和所有端口互通。

在 S1 上进行配置：
Switch(config)#isolate-port group test
Switch(config)#isolate-port group test switchport interface ethernet 1/0/1;1/0/10

第3章 端口环路检测功能操作配置

3.1 端口环路检测功能简介

随着交换机的发展，用户通过以太网交换机接入网络越来越多。在企业网中，用户通过二层以太网交换机接入网络，他们不仅有上 internet 的需求，同时内部二层互通的需求也相当迫切。当用户需要二层互通时，报文的转发直接通过 MAC 寻址，MAC 地址学习的正确与否决定着用户之间是否能够正确的互通。在二层交换中，通过 MAC 地址寻址来进行报文转发。二层设备的 MAC 地址学习都是通过源 MAC 地址学习来进行的。即：当端口收到一个未知源 MAC 地址的报文，会将这个 MAC 添加到接收端口上，以便后续以该 MAC 地址为目的的报文能够直接转发，即一次学习，多次转发。

当新来源 MAC 如果发现该 MAC 已经学习到了二层设备上，而源端口不一样，会修改原来 MAC 地址的源端口，也就是将原来的 MAC 地址移动到新的端口上来。因此当链路上存在环回情况时，最后会发现整个二层网络中的所有的 MAC 地址都移动到了存在环回的端口上了（大多情况是 MAC 地址频繁在不同端口间切换），导致二层网络瘫痪。在网络中进行端口环路检测非常必要，具有重要的意义。当设备通过环路检测发现了网络存在环回情况时，可以通过发送告警信息到网管系统，使网络管理人员能够及时发现网络中存在的问题，从而及时定位和解决。避免长时间的用户断网现象。

因为环路检测可以动态的发现链路上是否存在环回以及链路上的环回是否消失，因此，对于支持端口受控（比如端口隔离，端口 MAC 地址学习受控）的设备，可以实现自动维护。这样不仅减轻网管人员的工作负担，同时反应更加及时，能迅速将环回对网络的影响减小至最小。

3.2 端口环路检测功能配置任务序列

- 1. 配置环路检测的时间间隔
- 2. 启动端口环路检测功能
- 3. 配置端口环路控制方式
- 4. 显示和调试端口环路检测相关信息
- 5. 配置环路检测受控方式是否自动恢复

1. 配置环路检测的时间间隔

命令	解释
全局配置模式	
loopback-detection interval-time <loopback> <no-loopback> no loopback-detection interval-time	设置或恢复环路检测的时间间隔。

2. 启动端口环路检测功能

命令	解释
端口配置模式	

loopback-detection specified-vlan <vlan-list> no loopback-detection specified-vlan <vlan-list>	启动和关闭端口环路检测功能。
---	----------------

3. 配置端口环路控制方式

命令	解释
端口配置模式	
loopback-detection control {shutdown block learning } no loopback-detection control	打开和关闭端口的环路检测受控功能。

4. 显示和调试端口环路检测相关信息

命令	解释
特权配置模式	
debug loopback-detection no debug loopback-detection	打开端口环路检测功能模块的调试信息，本命令的 NO 操作关闭调试信息输出。
show loopback-detection [interface <interface-list>]	不输入参数则显示所有端口的环路检测状态和检测结果，输入参数则显示相应端口的状态和结果。

5. 配置环路检测受控方式是否自动恢复

命令	解释
全局配置模式	
loopback-detection control-recovery timeout <0-3600>	配置环路检测受控方式是否自动恢复或者恢复的时间间隔。

3.3 端口环路检测典型案例

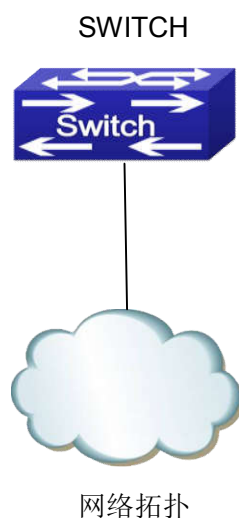


图 3-1 端口环路检测典型配置案例

上述配置中，交换机检测网络拓扑中是否存在环路情况。在交换机与外部网路连接的端口上启动端口环路检测功能，如果外部网络中存在环路的情况，交换机就会提示下连的网络存在环路，并将交换机上的这个端口控制，以免影响整个网络的正常工作。

SWITCH 配置任务序列：

```
Switch (config)#loopback-detection interval-time 35 15
```

```
Switch (config)#int 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
```

如果使用 block 控制，必须全局启动 mstp，并且配置生成树实例与 vlan 的对应关系

```
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 端口环路检测排错帮助

端口环路检测功能默认情况下是关闭的，如果需要检测环路可以打开该功能。

第4章 ULDP 操作配置

4.1 ULDP 功能简介

单向链路是网络中常见的一种错误链路状态，在光纤连接的链路中尤为常见。所谓单向链路，是指链路两端的端口之一可以收到对端发送的数据链路层报文，而对端不能收到本端发送的报文。此时链路物理层处于是连通状态，能正常工作，因而物理层的检测机制无法发现设备间通信存在问题。如下图所示，图中所示的光纤连接的错误就无法通过物理层的自动协商等机制发现。

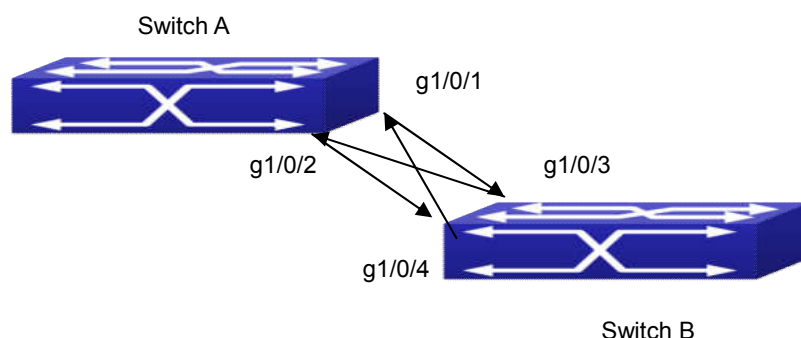


图 4-1 光纤交叉连接

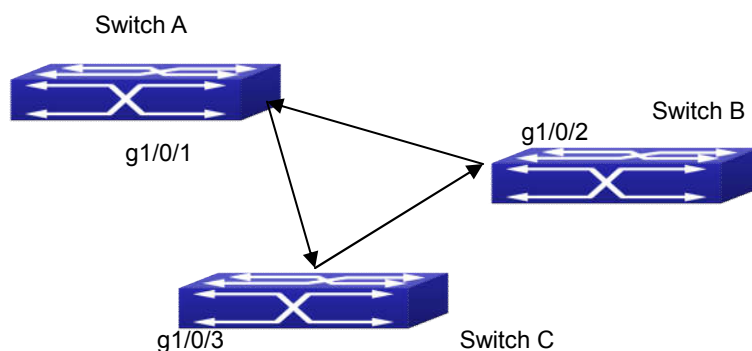


图 4-2 光纤一端未连接

这种情形通常会出现在以下几种情况之中：GBIC（Giga Bitrate Interface Converter，吉比特接口转换器）或接口出现故障、软件故障、硬件失效或其他异常表现。单向链路会引起一系列问题，比如生成树拓扑环路，广播黑洞等。

ULDP（UniDirectional Link Detection Protocol）有助于防止在上述几种失效中发生灾难性的事件，在通过光纤或铜质以太网线（例如超五类双绞线）连接的交换机上，它可以监控物理线路的链路状态，当发现单向链路后，向用户发送告警信息，并根据用户配置，自动或者手动地关闭相关端口。

神州数码系列交换机 ULDP 是通过交互 ULDP 报文识别对端设备，检测链路链接的正确性。端口使能了 ULDP 后，将启动协议状态机，在状态机的不同状态下发送不同类型的报文，与对端交互信息来检测链路的连接状况。ULDP 可以动态的学习对端的通告报文时间间隔，并以此来调整对端信息在本端的存活时间。此外，ULDP 还提供了重启机制，当端口被 ULDP 关闭后，可以通过重启机制来重新检测。其中，ULDP 发送通告报文的时间间隔和重启时间间隔可由用户配置，以便 ULDP 在不同的网络环境对链路的连接错误做出更快的响应。

ULDP 能正确工作的前提是链路工作在全双工方式，链路两端都使能了 ULDP 功能，认证方式和密码相同。

4.2 ULDP 配置任务序列

- 1. 启动全局 ULDP 功能
- 2. 启用端口 ULDP 功能
- 3. 配置全局积极模式
- 4. 配置端口积极模式
- 5. 配置关闭单向链路方式
- 6. 配置 Hello 报文时间间隔
- 7. 配置 Recovery 时间间隔
- 8. 重启被 ULDP 关闭的端口
- 9. 显示和调试 ULDP 相关信息

1. 启动全局 ULDP 功能

命令	解释
全局配置模式	
uldp enable uldp disable	全局启动或关闭 ULDP 功能。

2. 启动端口 ULDP 功能

命令	解释
端口配置模式	
uldp enable uldp disable	端口启动或关闭 ULDP 功能。

3. 配置全局积极模式

命令	解释
全局配置模式	

uldp aggressive-mode no uldp aggressive-mode	设置全局工作模式。
---	-----------

4. 配置端口积极模式

命令	解释
端口配置模式	
uldp aggressive-mode no uldp aggressive-mode	设置端口工作模式。

5. 配置关闭单向链路方式

命令	解释
全局配置模式	
uldp manual-shutdown no uldp manual-shutdown	配置关闭单向链路方式。

6. 配置 Hello 报文时间间隔

命令	解释
全局配置模式	
uldp hello-interval <integer> no uldp hello-interval	配置 Hello 报文时间间隔范围为 5—100 秒，默认为 10 秒。

7. 配置 Recover 时间间隔

命令	解释
全局配置模式	
uldp recovery-time <integer> no uldp recovery-time <integer>	配置端口重启时间间隔范围为 30—86400 秒，默认为 0 秒。

8. 重启被 ULDP 关闭的端口

命令	解释
全局配置模式或端口配置模式	
uldp reset	全局模式下重启所有端口； 端口模式下重启指定端口。

9. 显示和调试 ULDP 相关信息

命令	解释
特权模式	
show uldp [interface ethernet IFNAME]	显示 ULDP 信息。不带端口参数显示全局 ULDP 信息。带端口参数显示全局信息和该端口邻居信息。
debug uldp fsm interface ethernet <IFname> no debug uldp fsm interface ethernet <IFname>	打开或关闭指定端口的状态机迁移信息调试项。

debug uldp error no debug uldp error	打开或关闭错误信息调试项。
debug uldp event no debug uldp event	打开或关闭事件信息调试项。
debug uldp packet {receive send} no debug uldp packet {receive send}	打开或关闭所有端口收发报文类型。
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>	打开或关闭特定端口收发的某种类型报文的详细内容。

4.3 ULDP 功能典型案例

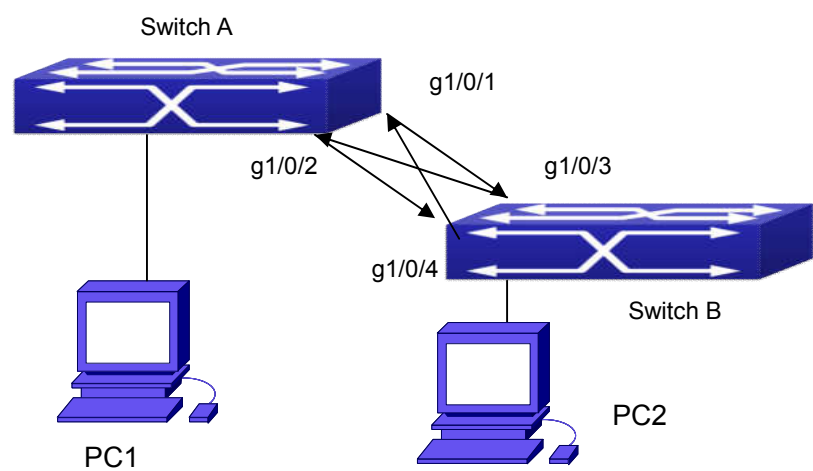


图 4-3 光纤交叉连接

在上述网络拓扑图中，SWITCH A 的端口 g1/0/1，g1/0/2 和 SWITCH B 的端口 g1/0/3，g1/0/4 均为光口，该连接为交叉连接。此时物理层连通，能工作正常，但是数据链路层异常。ULDP 可以检测并且关闭这种错误链路状态。最终的结果是 SWITCH A 的端口 g1/0/1，g1/0/2 和 SWITCH B 的端口 g1/0/3，g1/0/4 均被 ULDP 关闭。只有连接正确才能正常工作（不会被关闭）。

```
Switch A配置序列：
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配置序列:

```
SwitchB(config)#uldp enable
SwitchB(config)#interface ethernet 1/0/3
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
```

最终, SWITCH A的端口g1/0/1, g1/0/2均被ULDP关闭, 在PC1的CRT终端均有提示信息:

```
%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 shutted 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!
```

SWITCH B的端口g1/0/3, g1/0/4均被ULDP关闭, 在PC2的CRT终端均有提示信息:

```
%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 排错帮助

配置注意事项:

- ☞ 为了使得 ULDP 能够监测到光纤口上的一端未连或是交叉错连, 端口必须为全双工模式, 且速率相同。
- ☞ 当一端错连的光纤端口的自动协商机制在决定端口的工作模式和速度时, 即使 ULDP 已经使能, 也不起作用。在这种情况下, 认为该端口是 Down 的。
- ☞ 为了确保能正确的建立邻居和监测单向链路, 要求: 链路两端都使能 ULDP, 且认证模式和密码相同, 目前两端均不需验证密码。
- ☞ 发送 hello 报文的 hello interval 间隔可调 (默认 10 秒, 可调范围 5-100 秒), 以便根据不同的网络环境使 ULDP 对链路连接错误做出更快的响应。但是这个时间间隔必须小于 1/3 的 STP 收敛时间, 如果设置的时间过长, 在 ULDP 发现并关闭单向连接端口之前 STP loop 已经形成。反之, 如果设置的时间间隔太短, 端口的网络负担会增加, 带宽会减少。
- ☞ ULDP 不处理任何 LACP 事件, 把汇聚组 (如 Port-channel, trunk 端口等) 的每个链路看作是独立的, 分别进行处理。

- ☞ ULDP 不能和其它厂商相似的协议兼容，也就是说，不能在一端使能 ULDP，而在另一端使能其他的相似的协议。
- ☞ ULDP 功能默认是关闭的。打开全局 ULDP 功能后，可以同时打开调试开关来查看调试信息。设计了多条 **DEBUG** 命令来打印调试信息，如事件，状态机，错误，报文信息。对于报文信息，还可以分不同参数来打印不同类型的报文信息。
- ☞ **Recovery** 定时器 **timer** 默认不启用。只有用户配置了 **recovery time**（30-86400 秒）才启用。
- ☞ **reset** 命令和重启机制只能重启 ULDP 自动关闭的端口，被用户手工关闭的或是被其他模块关闭的端口不会被 ULDP 重新启动。

第5章 LLDP 功能操作配置

5.1 LLDP 功能简介

链路层发现协议（Link Layer Discovery Protocol, LLDP）是 802.1ab 中定义的新协议，它可使邻近设备向其他设备发出其状态信息的通知，并且所有设备的每个端口上都存储着定义自己的信息，如果需要还可以向与它们直接连接的近邻设备发送更新的信息，近邻的设备会将信息存储在标准的 SNMP MIBs。网络管理系统可从 MIB 处查询出当前第二层的连接情况。LLDP 不会配置也不会控制网络元素或流量，它只是报告第二层的配置。802.1ab 中的另一个内容是使网络管理软件利用 LLDP 所提供的信息去发现某些第二层的矛盾之处。IEEE 目前使用的是 IETF 现有的物理拓扑、接口和 Entity MIBs。

简单说来，LLDP 是一种邻近发现协议。它为以太网网络设备，如交换机、路由器和无线局域网接入点定义了一种标准的方法，使其可以向网络中其他节点公告自身的存在，并保存各个邻近设备的发现信息。例如设备配置和设备识别等详细信息都可以用该协议进行公告。

具体来说，LLDP 定义了一个通用公告信息集、一个传输公告的协议和一种用来存储所收到的公告信息的方法。要公告自身信息的设备可以将多条公告信息放在一个局域网数据包内传输，传输的形式为类型长度值（TLV）域。所有具备 LLDP 能力的设备必须支持设备机身 ID 和端口 ID 公告，但根据预计，多数设备还要支持系统名称、系统描述和系统能力公告。系统名称和系统描述公告可以为收集网络流量数据提供非常有用的信息。系统描述公告可以包含诸如公告设备的全名和系统的硬件类型及软件操作系统的版本信息等数据。

802.1AB 链接层发现协议（Link Layer Discovery Protocol），将能够使企业网络的故障查找变得更加容易，并加强网络管理工具在多厂商环境中发现和保持精确网络拓扑结构的能力。

许多网络管理软件都使用“自动发现”功能（Automated Discovery）来跟踪拓扑的变化和条件，但绝大多数软件最多也只是到达第三层，将设备分组到各个 IP 子网而已。但这些都是非常原始的数据，只是有关设备增加和移除的基本事件，而不是这些设备在哪里或怎样与网络服务进行操作等详情。

第二层发现（Layer 2 Discovery）则深度触及了诸如哪些设备附带有哪端口，以及哪些交换机与其他设备相互连接等信息，并显示出了客户端、交换机、路由器和应用服务器以及网络服务器之间的路径。如此详细的信息对计划和查询网络失败的根源将很有意义。

LLDP 将成为一种非常有用的管理工具，提供精确的网络映射、流量数据和网络故障查找信息。

5.2 LLDP 功能配置任务序列

1. 全局启动 LLDP 功能
2. 配置基于端口的 LLDP 功能开关
3. 配置端口 LLDP 运行状态
4. 配置 LLDP 更新报文发送间隔

5. 配置 LLDP 报文老化时间乘法器
6. 配置更新报文发送延迟
7. 配置 Trap 报文发送间隔
8. 配置端口使能 Trap 功能
9. 配置端口发送信息可选属性
10. 配置端口 Remote Table 存储空间大小
11. 配置端口 Remote Table 满时的操作类型
12. 显示和调试 LLDP 功能相关信息

1. 全局启动 LLDP 功能

命令	解释
全局配置模式	
lldp enable lldp disable	全局启动或关闭 LLDP 功能。

2. 配置基于端口的 LLDP 功能开关

命令	解释
端口配置模式	
lldp enable lldp disable	设置基于端口的 LLDP 功能开关。

3. 配置端口 LLDP 运行状态

命令	解释
端口配置模式	
lldp mode{send receive both disable}	设置指定端口 LLDP 运行状态。

4. 配置 LLDP 更新报文发送间隔

命令	解释
全局配置模式	
lldp tx-interval <integer> no lldp tx-interval	设置 LLDP 更新报文发送间隔为配置值或默认值。

5. 配置 LLDP 报文老化时间乘法器

命令	解释
全局配置模式	
lldp msgTxHold <value> no lldp msgTxHold	设置 LLDP 报文老化时间乘法器为配置值或默认值。

6. 配置更新报文发送延迟

命令	解释
全局配置模式	
lldp transmit delay <seconds> no lldp transmit delay	设置 LLDP 更新报文发送延迟为配置值或默认值。

7. 配置 Trap 报文发送间隔

命令	解释
全局配置模式	
lldp notification interval <seconds> no lldp notification interval	设置 Trap 报文发送间隔为配置值或默认值。

8. 配置端口使能 Trap 功能

命令	解释
端口配置模式	
lldp trap <enable disable>	设置端口使能 Trap 功能打开或关闭。

9. 配置端口发送信息可选属性

命令	解释
端口配置模式	
lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] no lldp transmit optional tlv	设置端口发送信息可选属性为选择值或默认值。

10. 配置端口 Remote Table 存储空间大小

命令	解释
端口配置模式	
lldp neighbors max-num <value> no lldp neighbors max-num	设置 Remote Table 存储空间大小为配置值或默认值。

11. 配置端口 Remote Table 满时的操作类型

命令	解释
端口配置模式	
lldp tooManyNeighbors {discard delete}	设置当 Remote Table 满时的操作类型。

12. 显示和调试 LLDP 功能相关信息

命令	解释
特权, 全局配置模式	
show lldp	显示当前 LLDP 配置信息。
show lldp interface ethernet <IFNAME>	显示当前端口 LLDP 配置信息。
show lldp traffic	显示各种计数器信息。
show lldp neighbors interface ethernet <IFNAME>	显示当端口 LLDP 的邻居信息。
show debugging lldp	显示所有开启 LLDP debug 开关的端口。
特权模式	

debug lldp no debug lldp	DEBUG 开关打开或关闭。
debug lldp packets interface ethernet <IFNAME> no debug lldp packets interface ethernet <IFNAME>	端口或全局 DEBUG 收发包信息功能打开或关闭。
端口配置模式	
clear lldp remote-table	清空端口 Remote-table。

5.3 LLDP 功能典型案例

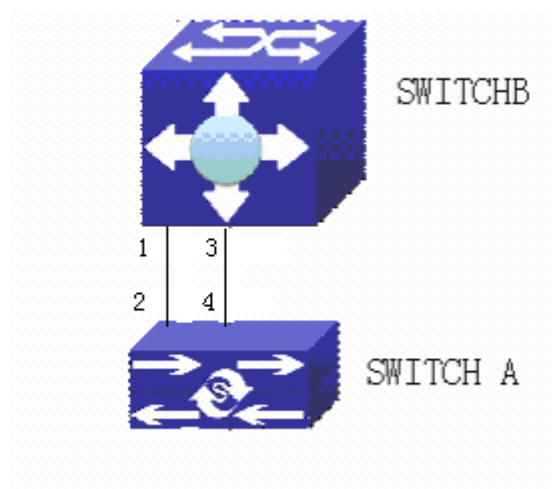


图 5-1 LLDP 功能典型配置案例

在上述网络拓扑图中, SWITCH B 的端口 1、3 与 SWITCH A 的端口 2、4 相连, SWITCH B 端口 1 配置了 LLDP 只接收报文模式, SWITCH A 的端口 4 配置了 Option TLV 为 portDes 和 SysCap。

SWITCH A 配置任务序列:

```
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 配置任务序列:

```
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 功能排错帮助

☞ LLDP 功能默认是关闭的。打开 LLDP 全局开关后, 可以同时打开调试关 debug lldp 来

查看调试信息。

- ☞ 使用 LLDP 功能的 **show** 功能可以看到全局或端口的配置信息。

第6章 Port Channel 配置

6.1 Port Channel 介绍

在介绍 Port Channel 之前，先介绍一下 Port Group 的概念：Port Group 是配置层面上的一个物理端口组，配置到 Port Group 里面的物理端口才可以参加链路汇聚，并成为 Port Channel 里的某个成员端口。在逻辑上，Port Group 并不是一个端口，而是一个端口序列。加入 Port Group 中的物理端口满足某种条件时进行端口汇聚，形成一个 Port Channel，这个 Port Channel 具备了逻辑端口的属性，才真正成为一个独立的逻辑端口。端口汇聚是一种逻辑上的抽象过程，将一组具备相同属性的端口序列，抽象成一个逻辑端口。Port Channel 是一组物理端口的集合体，在逻辑上被当作一个物理端口。对用户来讲，完全可以将这个 Port Channel 当作一个端口使用，因此不仅能增加网络的带宽，还能提供链路的备份功能。端口汇聚功能通常在交换机连接路由器、主机或者其他交换机时使用。

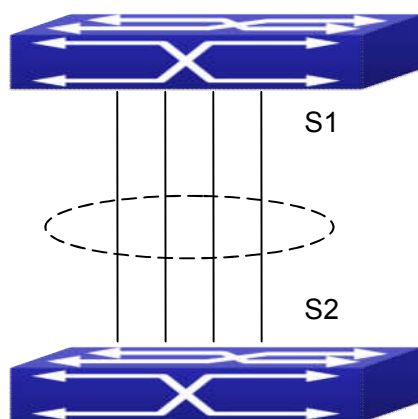


图 6-1 端口聚合示意图

如上图显示交换机 S1 的 1-4 号端口汇聚成一个 Port Channel，该 Port Channel 的带宽为 4 个端口带宽的总和。而 S1 如果有流量要经过 Port Channel 传输到 S2，S1 的 Port Channel 将根据流量的源 MAC 地址及目的 MAC 地址的最低位进行流量分配运算，根据运算结果决定由 Port Channel 中的某一成员端口承担该流量。当 Port Channel 中的一个端口连接失败，应该由该端口承担的流量将再次通过流量分配算法分配给其他连接正常的端口分担。流量分配算法由交换机的硬件决定。

交换机提供了两种配置端口汇聚的方法：手工生成 Port Channel、LACP（Link Aggregation Control Protocol）动态生成 Port Channel。只有双工模式为全双工模式的端口才能进行端口汇聚。

为使 Port Channel 正常工作，本交换机 Port Channel 的成员端口必须具备以下相同的属性：

- ☞ 端口均为全双工模式；
- ☞ 端口速率相同；
- ☞ 端口同为 Access 端口并且属于同一个 VLAN 或同为 Trunk 端口或同为 hybrid 端

口；

- ☞ 如果端口同为 Trunk 端口或同为 hybrid 端口，则其 Allowed VLAN 和 Native VLAN 属性也应该相同。

当交换机通过手工方式配置 Port Channel 或 LACP 方式动态生成 Port Channel，系统将自动选举出 Port Channel 中端口号最小的端口作为 Port Channel 的主端口（Master Port）。若交换机打开 Spanning-tree 功能，Spanning-tree 视 Port Channel 为一个逻辑端口，并且由主端口发送 BPDU 帧。

另外，端口汇聚功能的实现与交换机所使用的硬件有密切关系，本交换机支持任意两个相同属性的物理端口的汇聚，最大组数为 128 个，组内最多的端口数为 8 个。

汇聚端口一旦汇聚成功就可以把它当成一个普通的端口使用，在交换机中还建立了汇聚接口配置模式，与 VLAN 和物理接口配置模式一样，用户能在汇聚接口配置模式下对汇聚接口进行相关的配置。

6.2 LACP 简介

基于 IEEE802.3ad 标准的 LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚的协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路汇聚控制协议数据单元）与对端交互信息。

使能某端口的 LACP 协议后，该端口将通过发送 LACPDU 向对端通告自己的系统优先级、系统 MAC 地址、端口优先级、端口号和操作 Key。对端接收到这些信息后，将这些信息与其它端口所保存的信息比较以选择能够汇聚的端口，从而双方可以对端口加入或退出某个动态汇聚组达成一致。

操作 Key 是在端口汇聚时，LACP 协议根据端口的配置（即速率、双工、基本配置、管理 Key）生成的一个配置组合。

动态汇聚端口在使能 LACP 协议后，其管理 Key 缺省为零。静态汇聚端口在使能 LACP 后，端口的管理 Key 与汇聚组 ID 相同。

对于动态汇聚组而言，同组成员一定有相同的操作 Key，而手工和静态汇聚组中，Active 的端口有相同的操作 Key。

端口汇聚是将多个端口汇聚在一起形成一个汇聚组，以实现出/入负荷在汇聚组中各个成员端口中的分担，同时也提供了更高的连接可靠性。

6.2.1 静态 LACP 汇聚

静态 LACP 汇聚由用户手工配置，不使能 LACP 协议，在配置时是使用 on 模式强制端口进入汇聚组。

6.2.2 动态 LACP 汇聚

1. 动态 LACP 汇聚概述

动态 LACP 汇聚是一种系统自动创建/删除的汇聚，不允许用户增加或删除动态 LACP 汇聚中的成员端口。只有速率和双工属性相同、连接到同一个设备、有相同基本配置的端口

才能被动态汇聚在一起。即使只有一个端口也可以创建动态汇聚，此时为单端口汇聚。动态汇聚中，端口的 LACP 协议处于使能状态。

2. 动态汇聚组中的端口状态

在动态汇聚组中，端口可能处于两种状态：**selected** 或 **standby**。**selected** 端口和 **standby** 端口都能收发 LACP 协议，但 **standby** 端口不能转发用户报文。

由于设备所能支持的汇聚组中的最大端口数有限制，如果当前的成员端口数量超过了最大端口数的限制，则本端系统和对端系统会进行协商，根据设备 ID 优的一端的端口 ID 的大小，来决定端口的状态。具体协商步骤如下：

比较设备 ID（系统优先级+系统 MAC 地址）。先比较系统优先级，如果相同再比较系统 MAC 地址。设备 ID 小的一端被认为优。

比较端口 ID（端口优先级+端口号）。对于设备 ID 优的一端的各个端口，首先比较端口优先级，如果优先级相同再比较端口号。端口 ID 小的端口为 **selected** 端口，剩余端口为 **standby** 端口。

在一个汇聚组中，处于 **selected** 状态且端口号最小的端口为汇聚组的主端口，其他处于 **selected** 状态的端口为汇聚组的成员端口。

6.3 Port Channel 配置任务序列

- 1. 全局模式下建立一个 port group
- 2. 分别在端口模式下将这些端口加入指定的 group
- 3. 进入 port-channel 配置模式
- 4. 设置交换机的 load-balance 方式
- 5. 设置 LACP 协议的系统优先级
- 6. 设置 LACP 协议中当前端口的端口优先级
- 7. 设置 LACP 协议中当前端口的 Timeout 模式

1.创建 port group

命令	解释
全局配置模式	
port-group <port-group-number> no port-group <port-group-number>	创建或删除一个 port group。

2.把物理端口加入 port group

命令	解释
端口配置模式	
port-group <port-group-number> mode {active passive on} no port-group	把端口加入 port group，并设置模式。

3.进入 port-channel 配置模式

命令	解释
全局配置模式	
interface port-channel <port-channel-number>	进入 port-channel 配置模式。

4. 设置交换机的 load-balance 方式

命令	解释
全局配置模式	
load-balance {dst-src-mac dst-src-ip dst-src-mac-ip}	设置交换机的 load-balance，同时作用于 port-group 与 ECMP 功能。

5. 设置 LACP 协议的系统优先级

命令	解释
全局配置模式	
lacp system-priority <system-priority> no lacp system-priority	设置 LACP 协议的系统优先级，no 命令表示恢复为默认值。

6. 设置 LACP 协议中当前端口的端口优先级

命令	解释
端口配置模式	
lacp port-priority <port-priority> no lacp port-priority	设置当前端口 LACP 协议中的端口优先级，no 命令表示恢复为默认值。

7. 设置 LACP 协议中当前端口的 Timeout 模式

命令	解释
端口配置模式	
lacp timeout {short long} no lacp timeout	设置当前端口 LACP 协议中的端口 Timeout 模式，no 命令表示恢复为默认值。

6.4 Port Channel 举例

案例 1：以 LACP 方式配置 Port Channel。

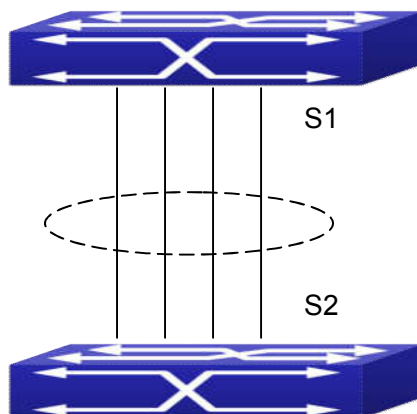


图 6-2 以 LACP 方式配置 Port Channel

如上图所示，交换机 S1 上的 1、2、3、4 端口都是 access 口，将这 4 个端口以 active 方式加入 group 1，交换机 S2 上 6、8、9、10 端口为 access 口，将这 4 个端口以 passive 方式加入 group 2，将以上对应端口分别用网线相连。

配置步骤如下：

```
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)#
```

配置结果：

过一段时间后，shell 提示端口汇聚成功，此时交换机 S1 的端口 1、2、3、4 汇聚成一个汇聚端口，汇聚端口名为 Port-Channel1，交换机 S2 的端口 6、8、9、10 汇聚成一个汇聚端口，汇聚端口名为 Port-Channel2，并且都可以进入汇聚接口配置模式进行配置。

案例 2：以 ON 方式配置 Port Channel。

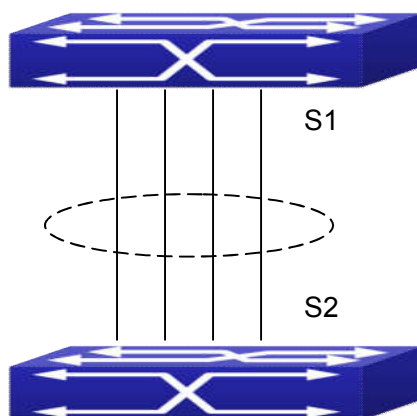


图 6-3 以 ON 方式配置 Port Channel

如图所示，交换机 S1 上的 1、2、3、4 端口都是 access 口，将这 4 个端口以 on 方式加入 group 1，在交换机 S2 上 6、8、9、10 端口为 access 口，将这 4 个端口以 on 方式加入 group 2。

配置步骤如下：

```
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
```

配置结果：

将交换机 S1 上的 1、2、3、4 端口依次加入 port-group1 后我们可以看到，以 on 方式加入

一个组完全是强制性的，两端的交换机并不会通过交换 LACP PDU 来完成汇聚，汇聚也是触发式的，当敲入将端口 1/0/2 加入 port-group1 的命令时，1 和 2 马上汇聚在一起形成 port-channel1，当将端口 1/0/3 加入 port-group1 时，1 和 2 汇聚成的 port-channel1 被拆散，马上 1、2、3 三个端口又重新汇聚成 port-channel1，当将端口 1/0/4 加入 port-group1 时，1、2、3 端口汇聚成的 port-channel1 被拆散，马上 1、2、3、4 端口又重新汇聚成 port-channel1（需要说明的是，当有一个新的端口要加入已经汇聚成功的组时，必须先拆散原先的组，然后再能汇聚成一个新的组）。结果是交换机 S1 和交换机 S2 上的三个端口都以 ON 模式汇聚起来，各自形成一个汇聚端口。

6.5 Port Channel 排错帮助

当配置端口聚合功能出现问题时，请检查是否是如下原因：

- ☞ 端口聚合组中的端口不具有相同的属性，即双工模式是否为全双工模式，速率是否强制成相同的速率，以及 VLAN 的属性等。如果检查不相同，则修改成相同。
- ☞ 一些命令不能在 port-channel 上的端口使用，包括：arp, bandwidth, ip, ip-forward 等。

第7章 MTU 配置

7.1 MTU 介绍

JUMBO（超大帧）在业界现在还没有一个确定的标准（包括帧格式和帧的长度），一般将大小在 1519—9000 之间的帧视为超大帧。超大帧的网络实现可以将整个网络的速度提高 2%到 5%。JUMBO 在使用上只是将交换机在收发的帧的长度增加了。但是考虑到 JUMBO 帧的长度问题，所以 JUMBO 是不送到 CPU 的，我们将送到 CPU 的 JUMBO 帧在收包处理中将 JUMBO 帧丢掉了。

7.2 MTU 配置任务序列

1. 配置 MTU 功能使能

1. 配置 MTU 功能使能

命令	解释
全局配置模式	
mtu [<mtu-value>]	启用 mtu 帧的收发功能。
no mtu	该命令的 NO 操作禁用 mtu 帧的收发功能。

第8章 EFM OAM 配置

8.1 EFM OAM 介绍

以太网最初为局域网而设计，但随着以太网的发展，应用扩展到了城域网和广域网，链路长度和网络规模上都迅速扩大，而由于有效管理维护机制的缺乏，严重阻碍以太网技术在城域网和广域网的应用。因此，在以太网上实现 OAM 功能成为必然的发展趋势。

关于以太网 OAM，有四个协议标准：802.3ah(EFM OAM)、802.3ag(CFM)、E-LMI、Y.1731；EFM OAM 和 CFM 为 IEEE 组织制定，EFM OAM 工作在数据链路层，可以有效地发现和管理底层存在的数据链路情况，利用 EFM OAM 技术可以有效提高对以太网的管理和维护能力，保障网络的稳定运行。CFM 为网络级以太网 OAM 技术，多应用于网络的接入汇聚层，用于监测整个网络的连通性、定位网络的连通性故障。Y.1731 是由 ITU，即国际电信联盟制定的标准，功能比 CFM 强大许多，也可以说 CFM 实现的功能是 Y.1731 的子集。E-LMI 是由 MEF 制定的标准，只应用于 UNI（用户边界和用户面对的供应商边界之间）。四个协议分别适用于不同的网络拓扑和管理要求，四者之间是互补的关系。

EFM OAM（Ethernet in the First Mile Operation, Administration and Maintenance，最后一英里以太网操作，管理和维护），工作在 OSI 模型的数据链路层，通过 OAM 子层来实现相关的功能，如下图所示：

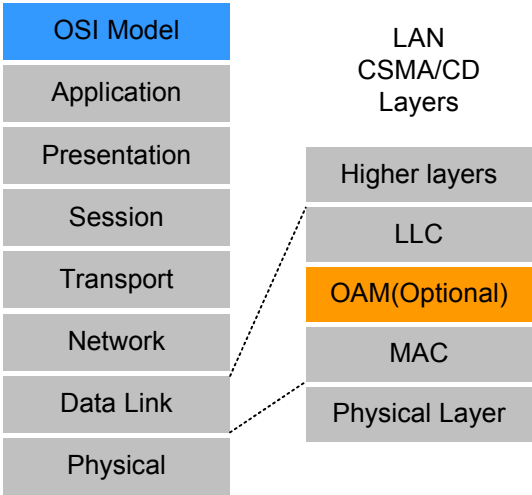


图 8-1 OAM 在 OSI 参考模型中的位置

OAM protocol data units(OAMPDU)使用慢协议的目的 mac 地址 01-80-c2-00-00-02，最大发送速率为 10Pkt/s。

EFM OAM 功能建立在 OAM 连接建立的基础上，提供了诸如链路监控，远端故障指示和远端环回控制等管理链路运行的一种机制，下面是 EFM OAM 工作流程的简单介绍。

1. 建立 OAM 连接

本端 OAM 实体通过交互 Information OAMPDU 发现远端 OAM 实体、并与之建立稳定

会话。EFM OAM 的工作模式有两种：主动模式、被动模式。EFM OAM 连接只能由主动模式的 OAM 实体发起，而被动模式的 OAM 实体只能等待对端 OAM 实体的连接请求。EFM OAM 连接建立后，两端的 OAM 实体通过持续发送 Information OAMPDU 保持连接。若在 5 秒钟内未收到对端 OAM 实体的 Information OAMPDU，则认为连接超时，OAM 连接中断。

2. 监控链路性能

以太网的故障检测非常困难，特别是在网络物理通信没有中断而网络性能缓慢下降的情况下。链路性能监控用于在各种环境下检测和发现链路层故障，EFM OAM 通过交互 Event Notification OAMPDU（事件通知报文）来监控链路：当一端 OAM 实体监控到一般链路事件时，将向其对端发送 Event Notification OAMPDU 进行通报，同时将监控信息记入日志并发送 SNMP Trap 上报网管系统；而对端 OAM 实体收到事件通知报文后，同样也将其记入日志并上报。这样，管理员就可以通过观察日志信息和网管系统动态地掌握网络的状况。

EFM OAM 监控的一般链路事件是指链路上发生的一般性错误事件，包括错误符号周期事件，错误帧事件，错误帧周期事件，错误帧秒总数事件。

错误符号周期事件：在指定 M 秒内，错误符号数大于或等于设定的低阈值。（符号：指物理介质上的最小数据传输单元。对于编码系统是唯一的，不同的物理介质上的 symbol 也可能是不同的。符号率即每秒电子状态改变的次数）

错误帧周期事件：指定帧数 N 为周期，在收到 N 个帧的周期内错误帧数大于或等于设定的低阈值。（错误帧：指收到的 CRC 检测出错的帧）

错误帧事件：在指定 M 秒内，收到的错误帧数大于或等于设定的低阈值。

错误帧秒总数事件：在指定 M 秒内，收到的错误帧秒数大于或等于设定的低阈值。（错误帧秒：某一秒内，收到至少 1 个错误帧，这一秒就称为错误帧秒）

3. 远端故障指示

由于设备故障或不可用而导致流量中断的情况，OAMPDU 定义了一个标志（即 Flags 域）允许以太网 OAM 实体将故障信息通知给对端。由于在以太网 OAM 连接已建立的情况下，两端的 OAM 实体会不断地交互 Information OAMPDU，因此本端 OAM 实体可以将本端发生的紧急链路事件通过 Information OAMPDU 告诉远端 OAM 实体，同时记录日志并发送 SNMP Trap 告警。这样，管理员可以通过观察日志信息和网管系统动态地了解链路状态，对相应的错误及时进行处理。

Information OAMPDU 将紧急链路事件即链路故障分为三种，分别是 Critical Event, Dying Gasp 和 Link Fault；不同厂商对这三种故障的具体定义都不同，我们的定义为：

Critical Event，端口 EFM OAM 功能关闭；

Link Fault，本地处于单向操作或错误数大于等于设定的高阈值；单向操作（Unidirectional Operation）是指在全双工且不支持自动协商的链路上，链路的一个方向无法工作（一般发生在通过光纤连接的链路上，收或发端因为某些原因无法连通）；EFM OAM 可以检测到该故障，并通过发送 Information OAMPDU 来通知远端 OAM 实体。

Dying Gasp，暂无定义；设备虽然不生成 Dying Gasp OAMPDU，但依然能够接收并处理对端发送的该类型 OAMPDU。

4. 远端环回

远端环回只有在以太网 OAM 连接建立完成后才能实现，且只有工作在 OAM 主动模式的端口才能发起环回请求。在 OAM 连接已经建立的情况下，主动模式的 OAM 实体发起远

端环回命令，对端实体对该命令进行响应。当远端处于环回模式下，除了 OAMPDU 报文以外的所有报文都将按照原路返回，网络管理员通过远端环回可以检测链路的延时，抖动和吞吐量。定期地进行环回检测可以及时发现网络故障，并通过分段环回检测来帮助定位故障发生的具体区域。注意，在远端环回模式下，将不能进行正常通信。

EFM OAM 典型应用拓扑如下图所示，它主要用于点到点链路和仿真点到点的 IEEE 802.3ah 链路，通过在两个点到点连接的设备上启用 EFM OAM 功能，监控以太网接入的“最后一英里”中常见的链路问题。用户端到电信运营商局端设备的这一段连接从使用者的角度看是“最前一英里”，而从运营者的角度则是“最后一英里”。

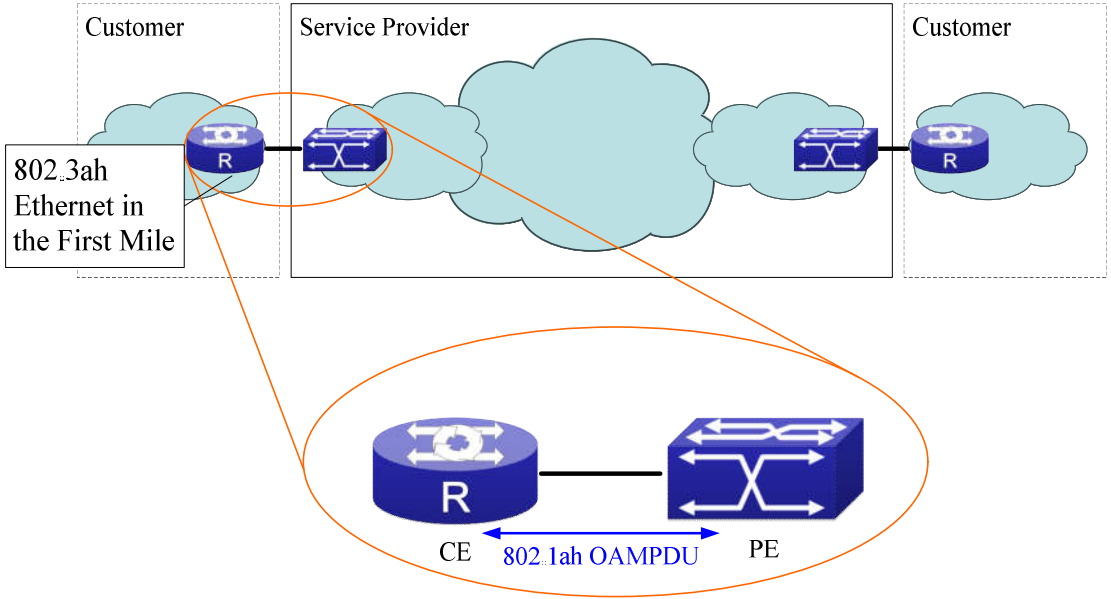


图 8-2 OAM 典型应用拓扑图

8.2 EFM OAM 基本配置

- EFM OAM 配置任务序列如下：
- 1.使能端口 EFM OAM 功能
 - 2.配置 EFM OAM 的链路监控（Link monitor）参数
 - 3.配置 EFM OAM 的远端错误指示（Remote Failure）参数
 - 4.使能端口 EFM OAM 环回功能
- 注意：配置 OAM 参数时，需要先启动 OAM 功能。

1. 使能端口 EFM OAM 功能

命令	解释
端口配置模式	
ethernet-oam mode {active passive}	配置 EFM OAM 的工作模式，默认为 active 主动模式。

ethernet-oam no ethernet-oam	使能端口 EFM OAM 功能；本命令的 no 操作为关闭端口 EFM OAM 功能。
ethernet-oam period <seconds> no ethernet-oam period	配置 OAMPDU 的发送周期（可选），本命令的 no 操作为恢复 OAMPDU 发送周期为默认值。
ethernet-oam timeout <seconds> no ethernet-oam timeout	配置 EFM OAM 连接超时时间（可选），本命令的 no 操作为恢复连接超时时间为默认值。

2. 配置 EFM OAM 的链路监控（Link monitor）参数

命令	解释
端口配置模式	
ethernet-oam link-monitor no ethernet-oam link-monitor	使能 EFM OAM 的链路监控功能（默认使能），本命令的 no 操作为关闭 EFM OAM 的链路监控功能。
ethernet-oam errored-symbol-period {threshold low <low-symbols> window <seconds>} no ethernet-oam errored-symbol-period {threshold low window }	配置错误符号周期事件的低阈值和窗口周期值；本命令的 no 操作为恢复各个配置为默认值。（可选）
ethernet-oam errored-frame-period {threshold low <low-frames> window <seconds>} no ethernet-oam errored-frame-period {threshold low window }	配置错误帧周期事件的低阈值和窗口周期值；本命令的 no 操作为恢复各个配置为默认值。（可选）
ethernet-oam errored-frame {threshold low <low-frames> window <seconds>} no ethernet-oam errored-frame {threshold low window }	配置错误帧事件的低阈值和窗口周期值；本命令的 no 操作为恢复各个配置为默认值。（可选）
ethernet-oam errored-frame-seconds {threshold low <low-frame-seconds> window <seconds>} no ethernet-oam errored-frame-seconds {threshold low window }	配置错误帧秒总数事件的低阈值和窗口周期值；本命令的 no 操作为恢复各个配置为默认值。（可选）

3. 配置 EFM OAM 的远端错误指示（Remote Failure）参数

命令	解释
端口配置模式	

ethernet-oam remote-failure no ethernet-oam remote-failure	使能 EFM OAM 的远端故障指示功能(故障指本地发生 critical-event 或 link-fault 事件), 本命令的 no 操作为关闭 EFM OAM 的远端故障指示功能。(可选)
ethernet-oam errored-symbol-period threshold high {high-symbols none} no ethernet-oam errored-symbol-period threshold high	配置错误符号周期事件的高阈值; 本命令的 no 操作为恢复配置为默认值。(可选)
ethernet-oam errored-frame-period threshold high {high-frames none} no ethernet-oam errored-frame-period threshold high	配置错误帧周期事件的高阈值; 本命令的 no 操作为恢复配置为默认值。(可选)
ethernet-oam errored-frame threshold high {high-frames none} no ethernet-oam errored-frame threshold high	配置错误帧事件的高阈值; 本命令的 no 操作为恢复配置为默认值。(可选)
ethernet-oam errored-frame-seconds threshold high {high-frame-seconds none} no ethernet-oam errored-frame-seconds threshold high	配置错误帧秒总数事件的高阈值; 本命令的 no 操作为恢复配置为默认值。(可选)

4. 使能端口 EFM OAM 环回功能

命令	解释
端口配置模式	
ethernet-oam remote-loopback no ethernet-oam remote-loopback	使能远端 EFM OAM 实体进入 OAM 环回模式(对端需要配置 OAM 环回支持), 本命令的 no 操作为取消远端的 OAM 环回。
ethernet-oam remote-loopback supported no ethernet-oam remote-loopback supported	使能端口的远端环回支持, 本命令的 no 操作为取消端口的远端环回支持。

8.3 EFM OAM 举例

案例:

在点到点链路的 CE 和 PE 设备上开启 EFM OAM 功能, 监控该“最后一英里”链路的性能, 当出现错误事件时, 会记录日志并上报网管系统; 在必要时, 可以使用远端环回功能检测链路。

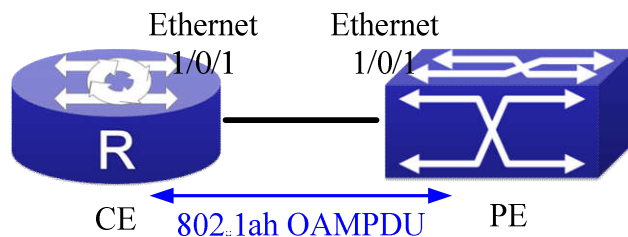


图 8-3 OAM 典型应用拓扑图

配置步骤：（下面省略了 SNMP 及 Log 的配置过程，具体请参考手册的相关内容）

在 CE 设备上的配置

```
CE(config)#interface ethernet 1/0/1
```

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

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

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

其他参数使用默认配置

在 PE 设备上的配置

```
PE(config)#interface ethernet 1/0/1
```

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

其他参数使用默认配置

当需要使用远端环回时，执行以下命令

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

检测完毕后，执行以下命令，使对端退出 OAM 环回

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

当不需要支持远端环回时，执行以下命令

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

8.4 EFM OAM 排错帮助

当在使用 EFM OAM 过程中遇到问题，请检查是否是如下原因：

- ✎ 检查链路两端的 OAM 实体是否都处于被动模式，都处于被动模式下的两个 OAM 实体之间无法建立 EFM OAM 连接。
- ✎ 请确保 SNMP 配置的正确性，否则错误事件无法上报网管系统。
- ✎ 处于 OAM 环回模式的链路，不能进行正常通信；在检测完链路的性能后，应该及时取消远端环回。
- ✎ 只有部分板卡支持远端环回功能，请确保所使用的板卡支持该功能。
- ✎ OAM 远端环回功能与 STP，MRPP，ULPP，Flow Control，loopback detection 功能互斥，因此开启了 OAM 环回功能的端口不能配置上述功能。
- ✎ 开启 OAM 时，会自动关闭端口的协商，故需确保链路对端的协商状态已关闭，对端未关闭协商会导致链路连接不成功；关闭 OAM 时，恢复端口的协商状态，确保链路两端协商状态一致，保证链路的正常。

- ✎ 开启 OAM 后，两端链路协商成功，UP 起来，将对端的 RX 方向光线拔下后，此时对端 TX 正常发光，开启 OAM 端的 RX 正常，故此时开启 OAM 的端口会一直处于 UP 状态。

第9章 bpdu-tunnel 配置

9.1 bpdu-tunnel 介绍

BPDU Tunnel 是一种二层隧道技术，它使不同地域私网用户的二层协议报文，通过修改源 MAC 地址的方式在运营商网络内的指定通道进行透明传输。

9.1.1 bpdu-tunnel 的作用

在城域网应用中，一个企业的多个分支机构可能会通过运营商网络进行互联。运营商通过提供 VPN 功能来使这些位于不同地理位置的网络组成一个“本地”局域网。这需要运营商网络提供“隧道”功能，即用户网络内产生的数据信息可以完整的通过运营商网络到达同一企业的其它网络。为了维持一个“本地”概念，不仅需要对于用户网络内的数据进行隧道传输，而且对于用于维护用户网络内的某些二层协议报文也要进行隧道传输。

9.1.2 bpdu-tunnel 的产生背景

在实际组网中，用户经常利用运营商提供的专线来构建自己的二层网络，这使同一用户的私网通常都分布在运营商公网的两侧。如下图所示，用户 A 拥有属于相同 VLAN 的两台设备 CE 1 和 CE 2，该用户的网络分为网络 1 和网络 2，二者通过运营商网络相连接。当二层协议报文在运营商网络中无法透传时，该用户的网络将无法独立进行二层协议的计算（如 STP 协议的生成树计算），从而与运营商网络的二层协议计算相互影响。

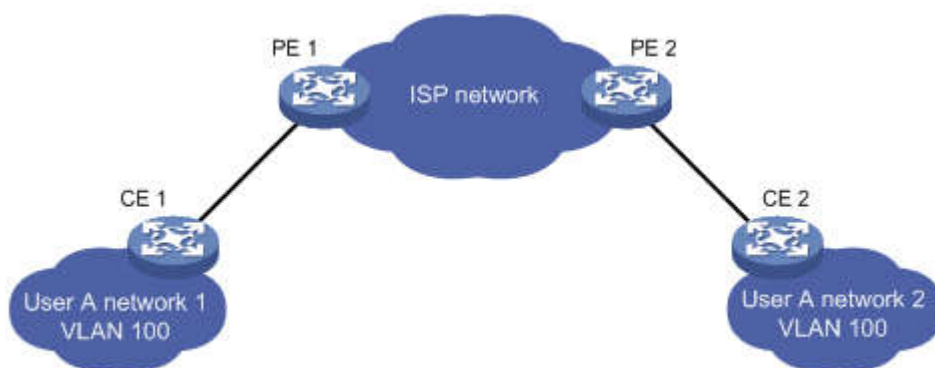


图 9-1 BPDU Tunnel 应用

9.2 bpdu-tunnel 配置任务序列

bpdu-tunnel 配置任务序列如下：

1. 配置全局隧道MAC地址
2. 配置端口支持隧道功能

1. 配置全局隧道 MAC 地址

命令	解释
全局配置模式	
bpdu-tunnel dmac <mac> no bpdu-tunnel dmac	配置或取消全局隧道 MAC 地址。

2. 配置端口支持隧道功能

命令	解释
端口配置模式	
bpdu-tunnel {stp gvrp uldp lacp dot1x} no bpdu-tunnel {stp gvrp uldp lacp dot1x}	开启或关闭端口上支持隧道功能

9.3 bpdu-tunnel 举例

典型应用场景如下图所示，在实际组网中，用户经常利用运营商提供的专线来构建自己的二层网络，这使同一用户的私网通常都分布在运营商公网的两侧。如图所示，用户 A 拥有属于相同 VLAN 的两台设备 CE 1 和 CE 2，该用户的网络分为网络 1 和网络 2，二者通过运营商网络相连接。当二层协议报文在运营商网络中无法透传时，该用户的网络将无法独立进行 二层协议的计算（如 STP 协议的生成树计算），从而与运营商网络的二层协议计算相互影响。

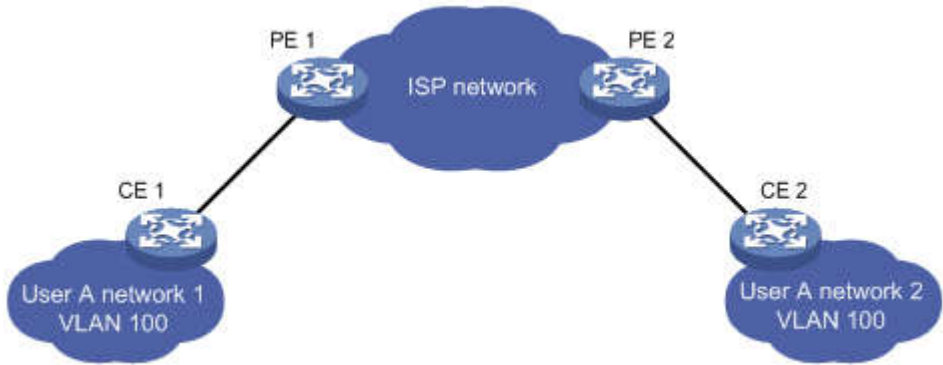


图 9-2 BPDU Tunnel 应用环境

利用 BPDU Tunnel 功能，可以在运营商网络中透传用户网络的二层协议报文：

1. 运营商网络一端的 PE 1 对从用户 A 的网络 1 收到的二层协议报文进行封装，将其目的 MAC 地址替换成一个特定的组播 MAC 地址，然后在运营商网络中进行转发；
2. 封装好的二层协议报文（称为 BPDU Tunnel 报文）被转发至运营商网络另一端的 PE 2，解封装后被还原为原始的目的 MAC 地址，并发送给用户 A 的网络 2。

边缘交换机 PE1 和 PE2 上关于 bpdu-tunnel 的配置如下：

PE1 的配置：

```
PE1(config)# bpdu-tunnel dmac 01-02-03-04-05-06
PE1(config-if-ethernet1/0/1)# bpdu-tunnel stp
PE1(config-if-ethernet1/0/1)# 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 的配置:
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
```

9.4 bpdu-tunnel 排错帮助

端口开启 stp, gvrp, uldp, lacp 和 dot1x 功能不能直接在该端口上配置 bpdu-tunnel 功能，需要在该端口上先关闭上述功能后才能配置 bpdu-tunnel 功能。

第10章 LLDP-MED

10.1 LLDP-MED 介绍

LLDP-MED（Link Layer Discovery Protocol-Media Endpoint Discovery）以 IEEE 的 802.1AB LLDP（Link Layer Discovery Protocol，链路层发现协议）为基础。LLDP 提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

802.1AB LLDP 中没有涉及到对语音设备信息的传输和管理。为了方便对网络中语音设备的部署和管理，LLDP-MED 对 LLDP 进行扩展，定义一些新的 TLV。新的 TLV 消息将提供 PoE（Power over Ethernet）、联网策略（Network Policy）以及紧急电话服务的介质端点位置等信息。

10.2 LLDP-MED 配置任务序列

1. LLDP-MED 基本功能配置

命令	解释
端口配置模式	
lldp transmit med tlv all no lldp transmit med tlv all	配置指定端口发送所有 LLDP-MED TLV 的功能。no 命令为关闭端口发送 LLDP-MED TLV 的功能。
lldp transmit med tlv capability no lldp transmit med tlv capability	配置指定端口发送 LLDP-MED Capability TLV。no 命令为关闭端口发送 LLDP-MED Capability TLV 的能力。
lldp transmit med tlv networkPolicy no lldp transmit med tlv networkPolicy	配置指定端口发送 LLDP-MED Network Policy TLV。no 命令为关闭端口发送 LLDP-MED Network Policy TLV 的能力。
lldp transmit med tlv extendPoe no lldp transmit med tlv extendPoe	配置指定端口发送 LLDP-MED Extended Power-Via-MDI TLV。no 命令为关闭端口发送 LLDP-MED Extended Power-Via-MDI TLV 的能力。

lldp transmit med tlv location no lldp transmit med tlv location	配置指定端口发送 LLDP-MED Location Identification TLV。no 命令为关闭端口发送 LLDP-MED Location Identification TLV 的能力。
lldp transmit med tlv inventory no lldp transmit med tlv inventory	配置端口发送 LLDP 报文时携带 LLDP-MED Inventory Management TLVs 集合。no 命令为关闭端口发送 LLDP-MED Inventory Management TLVs 的能力。
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}	配置端口的网络策略，包括端口的 VLAN ID、支持的应用（如语音和视频）、应用优先级以及使用策略等。
civic location {dhcp server switch endpointDev} <country-code> no civic location	配置 Civic Address LCI 格式地址的设备类型和国家编号，同时进入端口的 Civic Address LCI 格式地址配置模式，no 命令操作为取消端口 Civic Address LCI 格式地址的所有配置。
ecs location <tel-number> no ecs location	在端口上配置 ECS ELIN 格式的地址，no 命令操作取消在端口上已经配置的 ECS ELIN 格式的地址。
lldp med trap {enable disable}	配置指定端口使能或者禁止 LLDP-MED 网络拓扑发生变化发送 TRAP 消息功能。
Civic Address LCI 格式地址配置模式	
{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}	进入端口的 Civic Address LCI 格式地址配置模式后，配置详细的地址信息。

全局配置模式	
lldp med fast count <value> no lldp med fast count	LLDP-MED 快速启动机制激活的情况下，需要快速发送含有 LLDP-MED TLV 的 LLDP 报文，该命令对快速发送报文的个数进行设置。no 命令恢复快速发送报文的个数为默认值。
特权配置模式	
show lldp	显示全局 LLDP 和 LLDP-MED 的配置信息。
show lldp [interface ethernet <IFNAME>]	显示当前端口的 LLDP 和 LLDP-MED 配置信息。
show lldp neighbors [interface ethernet <IFNAME>]	显示端口邻居的 LLDP 和 LLDP-MED 信息。
show lldp traffic	显示端口 LLDP 和 LLDP-MED 收发包统计。

10.3 LLDP-MED 举例

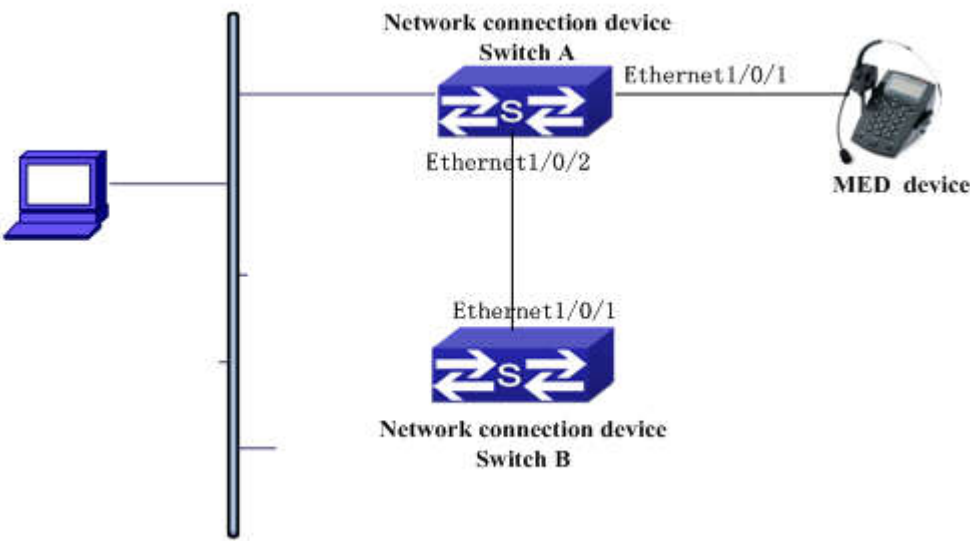


图 10-1 LLDP-MED 基本配置功能组网图

- 1) 配置 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 （本配置可省略，默认工作模式为 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) 配置 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) 验证配置结果

# 在 Switch A 上显示全局和接口的状态信息。

```
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
```

#### 说明:

- 1) switch A 的端口 2 和 switch B 的端口 1, 由于都是网络连接设备的端口, 不会主动发送含有 MED TLV 的 LLDP 报文, 所以尽管在 switch B 的端口 1 上配置发送 MED TLV, 该端口也不会发送 MED 相关信息, 导致该端口在 switch A 端口 2 上对应的 Remote 表项中没有 MED 相关信息。
- 2) LLDP-MED 端设备可以主动发送含有 MED TLV 的 LLDP 报文, 所以可以看到 MED 端设备在 switch A 端口 1 上对应的 Remote 表项含有 LLDP MED 信息。

## 10.4 LLDP-MED 排错帮助

当配置 LLDP-MED 功能出现问题时，请检查是否是如下原因：

- ✧ LLDP全局功能是否开启。
- ✧ 网络连接设备不会主动发送LLDP-MED TLV，只有在收到邻居MED设备发送的含有LLDP-MED TLV的LLDP报文后，才会发送LLDP-MED TLV。如果在网络连接设备上配置了发送LLDP-MED TLV的命令，端口在发送的报文中仍然不携带LLDP-MED TLV，就说明端口还未收到MED信息，端口发送LLDP-MED信息的功能还未使能。
- ✧ 如果邻居设备已经向网络连接设备发送了LLDP-MED信息，但是通过show lldp neighbors命令查看，没有显示LLDP-MED信息，说明邻居发送的LLDP-MED信息有误。

# 第11章 PORT SECURITY

## 11.1 PORT SECURITY 介绍

Port security 是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。这种机制通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备对网络的访问，通过检测从端口发出的数据帧中的目的 MAC 地址来控制非授权设备的访问。Port security 的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了 Port security 功能之后，当发现非法报文时，交换机将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。

## 11.2 PORT SECURITY 配置任务序列

### 1.PORT SECURITY 基本功能配置

| 命令                                                                                                                                                                                  | 解释                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 端口配置模式                                                                                                                                                                              |                                                                                                             |
| <b>switchport port-security</b><br><b>no switchport port-security</b>                                                                                                               | 配置端口的 port-security 功能。                                                                                     |
| <b>switchport port-security mac-address &lt;mac-address&gt; [vlan &lt;vlan-id&gt;]</b><br><b>no switchport port-security mac-address &lt;mac-address&gt; [vlan &lt;vlan-id&gt;]</b> | 配置端口的静态安全 MAC。                                                                                              |
| <b>switchport port-security maximum &lt;value&gt; [vlan &lt;vlan-list&gt;]</b><br><b>no switchport port-security maximum &lt;value&gt; [vlan &lt;vlan-list&gt;]</b>                 | 配置端口允许的最大安全 MAC 地址数。                                                                                        |
| <b>switchport port-security violation {protect   recovery   restrict   shutdown}</b><br><b>no switchport port-security violation</b>                                                | 当超过设定 MAC 地址数量的最大值，或访问该端口的设备 MAC 地址不是这个 MAC 地址表中该端口的 MAC 地址，或同一个 VLAN 中一个 MAC 地址被配置在几个端口上时，就会引发违反 MAC 地址安全。 |
| <b>switchport port-security aging {static   time &lt;value&gt;   type {absolute   inactivity}}</b><br><b>no switchport port-security violation aging {static   time   type}</b>     | 本命令用来使能端口的 port-security 老化表项的功能，指定老化时间以及类型等。                                                               |
| 特权配置模式                                                                                                                                                                              |                                                                                                             |
| <b>clear port-security {all   configured   dynamic   sticky} [[address &lt;mac-addr&gt;   interface</b>                                                                             | 本命令用来清除端口的安全 MAC 表项。                                                                                        |

|                                                                                       |                        |
|---------------------------------------------------------------------------------------|------------------------|
| <code>&lt;interface-id&gt; [vlan &lt;vlan-id&gt; ]</code>                             |                        |
| <code>show port-security [interface &lt;interface-id&gt;]<br/>[address   vlan]</code> | 显示 port-security 配置信息。 |

## 11.3 PORT SECURITY 举例

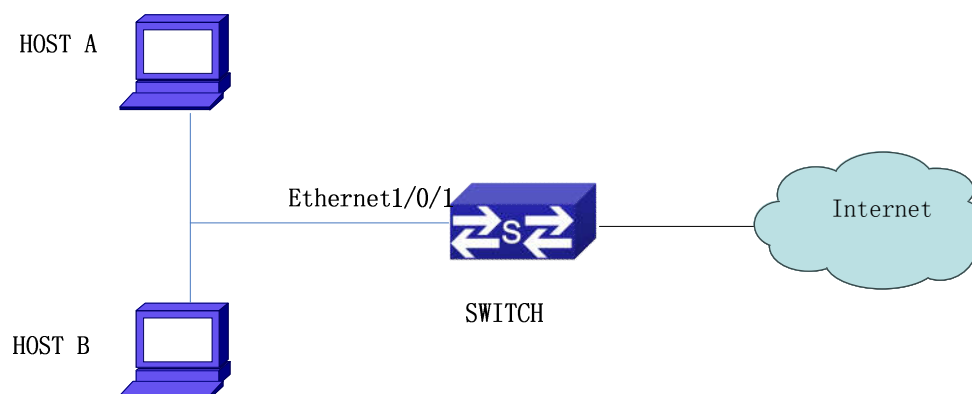


图 11-1 Port security 功能典型组网图

在交换机端口启动 Port security 功能时，配置端口允许的最大安全 MAC 数量为 10，该端口最多只允许 10 个用户接入 Internet，超过最大数量后，新来的用户无法访问 Internet，既可以限制用户的数量又起到安全访问的功能。如果配置端口允许的最大安全 MAC 数量为 1，则只允许一个用户访问，HOST A 和 B 只有一个能访问网络。

配置步骤：

#配置交换机 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)#
```

## 11.4 PORT SECURITY 排错帮助

当配置 PORT SECURITY 功能出现问题时，请检查是否是如下原因：

- ☞ 功能是否正常开启
- ☞ 是否配置了允许的最大MAC数量

## 第12章 DDM 配置

### 12.1 DDM 介绍

#### 12.1.1 DDM 简介

DDM 即数字诊断监测 (Digital Diagnostic Monitor)，在 SFF-8472 MSA 中，规范了数字诊断功能的详细内容。该规范规定，在模块内部的电路板上侦测和数字化参数信号；然后，提供经过标定的结果或提供数字化的测量结果及标定参量，这些信息被存贮在标准的内存结构中，以便通过双缆串行接口读取。

在通常我们所说的智能光模块上均支持数字诊断功能。通过光模块内部的 MCU，网络管理单元可以实时的监测光模块的温度 (temperature)、工作电压 (voltage)、激光偏置电流 (bias current) 以及发射光功率 (tx power) 和接收光功率 (rx power)，获取光模块各参数的阈值，并能得到当前光模块的实时状态。通过这些手段，可以帮助网络管理单元找出光纤链路中发生故障的位置，简化维护工作，提高系统的可靠性。

光接口交换机的数字诊断功能 (DDM) 是运营商客户的基本需求，可做以下应用：

##### 1、模块寿命预测

通过监测激光的偏置电流来预测激光器的寿命，可以粗略的估计激光器的使用寿命是否接近终了。通过对收发模块内部的工作电压和温度进行实时监测，可以让系统管理员发现一些潜在的问题：

- (1) Vcc 电压过高，会带来 CMOS 器件的击穿，Vcc 电压过低，激光器不能正常工作；
- (2) 接收功率太高，会损坏接收模块；接收功率过低，接收模块断路不能正常工作；
- (3) 工作温度太高，会加速器件的老化；
- (4) 通过对接收到的光功率的监测，可以对线路和远端发射机的性能进行监控。

##### 2、故障定位

在光链路中，定位故障的发生位置对业务的快速加载至关重要。故障隔离特性则可以使系统管理员快速定位链路故障的位置。此特性可以定位故障是在模块内还是在线路上，是在本地模块还是在远端模块。通过快速定位故障，减少了系统的故障修复时间。

通过数字诊断功能，对温度 (temperature)、工作电压 (voltage)、激光偏置电流 (bias current) 以及发射光功率 (tx power) 和接收光功率 (rx power) 的警告 (warning) 和警报 (alarm) 状态进行综合分析，可以快速的定位故障。状态变量 Tx Fault (发射失败) 和 Rx LOS (接收信号丢失) 等状态都对故障的分析起着重要的作用。

##### 3、兼容性验证

兼容性验证就是分析模块的工作环境是否符合数据手册或和相关的标准兼容。模块的性能只有在这种兼容的工作环境下才能得到保证。在有些情况下，由于环境参数超出数据手册或相关的标准，将造成模块性能下降，从而出现传输误码。工作环境与模块不兼容的情况有：

- (1) 电压超出规定范围；
- (2) 接收光功率过载或低于接收机灵敏度；
- (3) 温度超出工作温度范围。

12.1.2 DDM 功能

DDM 功能描述具体如下：

1. 显示收发器的监测信息

收发器的实时参数有发射功率（TX power）、接收功率（RX power）、温度（Temperature）、电压（Voltage）、偏置电流（Bias current），通过对这些参数的检测以及对警告（warning）、报警（alarm）、实时状态、阈值等相关监测信息的查询，网络管理员可以了解到当前收发器的工作状态，发现一些潜在的问题。通过查看光模块的故障信息可以帮助网络管理员快速定位线路故障，加快修复故障的时间。

2. 用户自定义阈值

收发器对于实时参数 TX power、RX power、Temperature、Voltage、Bias current 有固定的阈值，但由于用户的使用环境不一样，需要自定义阈值来监测收发器的工作状态，因此，通过自定义阈值，可以让用户灵活的监测收发器的工作状态，及时的发现故障。阈值类型包括报警的高阈值（high alarm）、报警的低阈值（low alarm）、警告的高阈值（high warn）、警告的低阈值（low warn）。

用户配置的阈值和厂商配置的阈值可以同时显示出来，供用户查看。当用户定义的阈值不合理时，会提示用户，并自动按厂商的阈值进行报警或警告。用户可以恢复所有阈值为厂商阈值，可以恢复单个阈值为厂商阈值。

阈值的合理性：报警的高低阈值应该包含警报的高低阈值，并且高阈值应该大于低阈值，即 high alarm>= high warn>= low warn>= low alarm。

对于 sfp 光模块，接收功率的校验方式分内部校验和外部校验，这个是厂商决定的。参数的实时监测值和厂商预设的阈值采用相同的校验方式。

3. 软件监控

用户除了实时的查看收发器模块的工作状态，还需要监控之前收发器发生异常时的时间、异常类型等详细情况。软件监控这个功能可以让用户通过查看日志发现之前收发器产生的异常情况，也可以让用户通过命令查询上一次的发生异常的详细情况。当用户发现光模块有异常信息，对其进行处理后，需要重新监控光模块的信息时，可以清楚软件监控的异常信息，重新开始监控。

12.2 DDM 配置任务序列

DDM 配置任务序列如下：

- 1. 显示收发器（transceiver）实时检测信息
- 2. 配置收发器（transceiver）各监测参数的报警或警告阈值
- 3. 配置收发器（transceiver）的软件监控状态
  - （1）配置收发器（transceiver）的软件监控的时间间隔
  - （2）配置收发器（transceiver）的软件监控的使能状态
  - （3）显示收发器（transceiver）的软件监控信息
  - （4）清除收发器（transceiver）的软件监控信息

1. 显示收发器（transceiver）实时检测信息

| 命令               | 解释 |
|------------------|----|
| 用户模式、特权模式、全局配置模式 |    |

|                                                                              |             |
|------------------------------------------------------------------------------|-------------|
| <b>show transceiver [interface ethernet &lt;interface-list&gt;] [detail]</b> | 显示收发器的监测信息， |
|------------------------------------------------------------------------------|-------------|

## 2. 配置收发器（transceiver）各监测参数的报警或警告阈值

| 命令                                                                                                                                                                      | 解释          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 端口配置模式                                                                                                                                                                  |             |
| <b>transceiver threshold {default   {temperature   voltage   bias   rx-power   tx-power} {high-alarm   low-alarm   high-warn   low-warn} {&lt;value&gt;   default}}</b> | 用户配置自定义的阈值。 |

## 3. 配置收发器（transceiver）的软件监控状态

### (1) 配置收发器（transceiver）的软件监控的时间间隔

| 命令                                                                                            | 解释                                          |
|-----------------------------------------------------------------------------------------------|---------------------------------------------|
| 全局配置模式                                                                                        |                                             |
| <b>transceiver-monitoring interval &lt;minutes&gt;<br/>no transceiver-monitoring interval</b> | 设置软件监控的时间间隔。本命令的 no 命令为设置时间间隔为默认时间间隔 15 分钟。 |

### (2) 配置收发器（transceiver）的软件监控的使能状态

| 命令                                               | 解释                                                                   |
|--------------------------------------------------|----------------------------------------------------------------------|
| 端口配置模式                                           |                                                                      |
| <b>transceiver-monitoring {enable   disable}</b> | 设定端口是否开启软件监控功能。只有开启软件监控任务的端口，系统才会记录其异常状态。当端口关闭了软件监控任务后，此端口的异常信息将被清空。 |

### (3) 显示收发器（transceiver）的软件监控信息

| 命令                                                                                      | 解释                                              |
|-----------------------------------------------------------------------------------------|-------------------------------------------------|
| 特权模式、全局配置模式                                                                             |                                                 |
| <b>show transceiver threshold-violation [interface ethernet &lt;interface-list&gt;]</b> | 显示软件监控信息，包括上一次超过阈值的信息、当前软件监控的时间间隔和该端口是否使能了软件监控。 |

### (4) 清除收发器（transceiver）的软件监控信息

| 命令                                                                                       | 解释             |
|------------------------------------------------------------------------------------------|----------------|
| 特权模式                                                                                     |                |
| <b>clear transceiver threshold-violation [interface ethernet &lt;interface-list&gt;]</b> | 清空软件监控的阈值异常信息。 |

## 12.3 DDM 举例

举例 1:

在交换机上的 21 口和 23 口插上支持 DDM 的 SFP 光模块, 在 24 口上插上不支持 DDM 的 SFP 光模块, 22 口不插任何 SFP 光模块, 显示光模块的 DDM 信息。

a、显示所有正常读取出实时参数的端口信息 (不支持或者没有插光模块, 则不显示), 例如:

Switch#show transceiver

| Interface | Temp (°C) | 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、显示指定端口的信息(不支持或没插光模块的显示 N/A), 例如:

Switch#show transceiver interface ethernet 1/0/21-22;23

| Interface | Temp (°C) | 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、显示详细的信息, 包括端口的基本信息、实时监测参数值、警告 (warning)、报警 (alarm)、异常状态、阈值信息、序列号, 例如:

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. Serial Number is 1108000001.

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 (°C)  | 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. Serial Number is 1108000001.

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

说明：如果序列号全为 0，表示序列号没有指定，则显示为：

SFP found in this port, manufactured by company, on Sep 29 2010.

Type is 1000BASE-SX. Serial Number is not specified.

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.

举例 2:

在交换机上的 21 口插上支持 DDM 的 SFP 光模块，显示光模块的 DDM 信息后配置光模块的阈值。

步骤 1：显示光模块的 DDM 详细信息

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 (°C)  | 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   |

步骤 2：配置光模块的发送功率阈值，警告下限阈值为-12，报警下限阈值为-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

步骤 3: 显示光模块的 DDM 详细信息。报警采用用户配置的阈值，厂商设置的阈值用括号标注起来，由于  $-13.01 < -12.00$ ，所以发送功率有 (A-) 的报警。

```
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 (°C)  | 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) |

举例 3:

在交换机上的 21 口插上支持 DDM 的 SFP 光模块，显示光模块的软件监控信息后使能端口的软件监控功能。

步骤 1: 显示光模块的软件监控信息。21 口和 22 口都没有使能软件监控功能，软件监控的时间间隔是 30 分钟。

```
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.

步骤 2: 使能 21 口的软件监控功能。

```
Switch(config)#interface ethernet 1/0/21
```

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

步骤 3: 显示光模块的软件监控信息。从显示可以看到，21 口使能了软件监控功能，上一次超过阈值出现报警的时间是 2011 年 1 月 2 日的 11 点零 50 秒，超过阈值时详细的 DDM 信息也显示了出来。

```
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 (°C)  | 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.

## 12.4 DDM 排错帮助

当在使用 DDM 功能的过程中遇到问题，请检查是否是如下原因：

- ☞ 请确保端口上的光模块收发器已经插紧，否则无法显示 DDM 信息（显示为 N/A 或没有 DDM 信息）；
- ☞ 请确保 SNMP 配置的正确性，否则报警事件无法上报网管系统；
- ☞ 只有部分板卡和盒式交换机支持 SFP 的 DDM 功能或 XFP 的 DDM 功能，请确保所使用的板卡和盒式交换机支持相应的功能；
- ☞ 使用 **show transceiver** 命令或 **show transceiver detail** 命令时，交换机要检查所有端口，所以显示的时间会比较慢，建议查询指定端口上收发器的监测信息。
- ☞ 请确保用户自定义的阈值的正确性，当任意一个阈值设置错误时，收发器将自动按照厂商的设置的方式进行报警。