JXNET 申信

JX S2700 非网管系列 以太网交换机
配置指南(CLI)
(Rel_02)

北京甲信技术有限公司（以下简称“甲信”）为客户提供全方位的技术支持和服务。直接向甲信购买产品的用户，如果在使用过程中有任何问题，可与甲信各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于甲信产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：　　www.jiaxinnet.com.cn

技术支持邮箱：　jxhelp@bjjx.cc

技术支持热线：　400-179-1180

公司总部地址：　北京市海淀区丹棱 SOHO 7 层 728 室

邮政编码:　　100080

声　明

Copyright ©2025

北京甲信技术有限公司

版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

JXNET 甲信是北京甲信技术有限公司的注册商标。

对于本手册中出现的其它商标，由各自的所有人拥有。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前 言

概述

本文档系统介绍了 JX S2700(A)系列以太网交换机（以下简称 JX S2700 系列）设备支持的特性及其相关配置。主要内容包括基础配置、以太网、环网保护、IP 业务、PoE、DHCP、可靠性、安全性、QoS 等基本原理和配置过程，并提供相关的配置案例。在本文档的附录中，提供了该文档所涉及的术语和缩略语。

阅读本文档有助于读者系统掌握设备的原理和各种配置信息，以及如何应用该设备进行组网。

产品版本

与本文档相对应的产品版本如下所示。

产品名称	软件版本	硬件版本
JX S2700 系列以太网交换机	V7.01	A

约定

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

符号	说明
	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级标题、二级标题、三级标题、Block 采用**黑体**表示。
楷体	警告、提示等内容用楷体表示。
“Lucida Console”格式	“Lucida Console”格式表示屏幕输出信息。此外，屏幕输出信息中夹杂的用户从终端输入的信息采用加粗字体表示。

命令行格式约定

格式	说明
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**粗体**表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 02 (2024-07-05)

第二次正式发布。

文档版本 01 (2023-12-10)

第一次正式发布。

目 录

1 基础配置 1
1.1 登录设备 1
1.1.1 简介 1
1.1.2 通过 Console 口登录设备 2
1.1.3 通过 Telnet 登录设备 4
1.1.4 通过 SSH 登录设备 7
1.1.5 通过 Web 登录设备 9
1.1.6 管理登录用户 10
1.1.7 用户密码恢复 12
1.1.8 终端属性设置 12
1.1.9 Bootrom 密码设置 13
1.1.10 登录方式修改（弱口令漏洞解决方案） 13
1.2 加载与升级 15
1.2.1 简介 15
1.2.2 通过 TFTP 命令行升级方式升级系统软件 15
1.2.3 通过 FTP 命令行升级方式升级系统软件 16
1.2.4 检查配置 16
1.2.5 指定系统启动镜像 16
1.2.6 检查系统版本信息 16
1.3 时间管理 17
1.3.1 简介 17
1.3.2 配置准备 19
1.3.3 缺省配置 19
1.3.4 配置 NTP 20
1.3.5 检查配置 22
1.3.6 配置 NTP 功能示例 22
1.4 PTP 24
1.4.1 简介 24
1.4.2 缺省配置 25
1.4.3 配置全局属性 26
1.4.4 配置接口属性 26
1.5 接口管理 27

1.5.1 简介 27
1.5.2 接口的缺省配置 27
1.5.3 配置接口基本属性 28
1.5.4 配置接口信息统计功能 29
1.5.5 配置接口流控功能 29
1.5.6 配置接口打开或关闭 30
1.5.7 配置接口允许通过的 tagged 报文类型 30
1.5.8 配置管理报文优先级 30
1.5.9 查看接口统计 31
1.5.10 检查配置 31
2 以太网 1
2.1 MAC 地址转发表 1
2.1.1 简介 1
2.1.2 配置准备 3
2.1.3 MAC 地址转发表的缺省配置 4
2.1.4 配置静态 MAC 地址 4
2.1.5 配置黑洞 MAC 地址 4
2.1.6 配置 MAC 地址学习 5
2.1.7 配置基于 VLAN 的 MAC 地址学习 5
2.1.8 配置 MAC 地址学习数目限制 5
2.1.9 配置 MAC 老化时间 5
2.1.10 配置 MAC 地址漂移检测与保护 6
2.1.11 检查配置 6
2.1.12 维护 7
2.1.13 配置 MAC 地址转发表示例 7
2.2 VLAN 9
2.2.1 简介 9
2.2.2 配置准备 11
2.2.3 VLAN 的缺省配置 11
2.2.4 配置 VLAN 属性 12
2.2.5 配置接口模式 12
2.2.6 配置基于 Access 接口的 VLAN 12
2.2.7 配置基于 Trunk 接口的 VLAN 13
2.2.8 配置基于 Hybrid 接口的 VLAN 14
2.2.9 配置基于 MAC 地址的 VLAN 14
2.2.10 配置基于 IP 子网的 VLAN 15
2.2.11 配置基于协议的 VLAN 15
2.2.12 检查配置 16
2.2.13 查询 VLAN 统计信息 16

2.2.14 配置 VLAN 示例 17
2.3 Voice VLAN 19
2.3.1 简介 19
2.3.2 配置准备 20
2.3.3 Voice VLAN 的缺省配置 20
2.3.4 配置 OUI 地址 21
2.3.5 使能 Voice VLAN 功能 21
2.3.6 检查配置 22
2.3.7 配置端口加入 Voice VLAN 示例 22
2.3.8 配置 LLDP 实现 IP 话机接入 Voice VLAN 示例 23
2.4 QinQ 24
2.4.1 简介 24
2.4.2 配置准备 25
2.4.3 QinQ 的缺省配置 26
2.4.4 配置基本 QinQ 26
2.4.5 配置灵活 QinQ 27
2.4.6 配置网络侧接口为 Trunk 模式 28
2.4.7 配置 TPID 28
2.4.8 检查配置 28
2.4.9 配置基本 QinQ 示例 29
2.4.10 配置灵活 QinQ 示例 30
2.5 VLAN 转换 31
2.5.1 简介 31
2.5.2 配置准备 32
2.5.3 VLAN 转换的缺省配置 32
2.5.4 配置 VLAN 转换 33
2.5.5 检查配置 33
2.5.6 配置 VLAN 转换示例 34
2.6 MRP/MVRP 35
2.6.1 简介 35
2.6.2 配置准备 37
2.6.3 缺省配置 38
2.6.4 配置 MVRP 基本功能 38
2.6.5 检查配置 38
2.6.6 配置 MVRP 应用示例 39
3 IP 业务 1
3.1 IP 基础配置 1
3.1.1 简介 1
3.1.2 配置准备 1

3.1.3 VLAN 接口的缺省配置 1
3.1.4 配置 VLAN 接口 IPv4 地址 2
3.1.5 配置 VLAN 接口 IPv6 地址 2
3.1.6 检查配置 3
3.1.7 配置 VLAN 接口 IP 地址实现和主机互通示例 3
3.2 LOOPBACK 接口 4
3.2.1 简介 4
3.2.2 配置准备 5
3.2.3 LOOPBACK 接口的缺省配置 5
3.2.4 配置 LOOPBACK 接口 IP 地址 5
3.2.5 检查配置 5
3.3 SLAAC 6
3.3.1 简介 6
3.3.2 配置准备 6
3.3.3 SLAAC 的缺省配置 6
3.3.4 使能 SLAAC 6
3.3.5 配置 SLAAC 示例 6
3.4 ARP 7
3.4.1 简介 7
3.4.2 配置准备 7
3.4.3 ARP 的缺省配置 7
3.4.4 配置静态 ARP 表项 8
3.4.5 配置动态 ARP 表项 8
3.4.6 检查配置 8
3.4.7 维护 8
3.4.8 配置 ARP 示例 9
3.5 NDP 10
3.5.1 简介 10
3.5.2 配置准备 11
3.5.3 NDP 的缺省配置 11
3.5.4 配置静态邻居表项 11
3.5.5 配置动态 NDP 老化时间 12
3.5.6 检查配置 12
3.5.7 维护 12
3.6 静态路由 13
3.6.1 简介 13
3.6.2 配置准备 13
3.6.3 配置静态路由 13
3.6.4 检查配置 14
3.6.5 配置静态路由示例 14

3.7 策略路由 15
3.7.1 简介 15
3.7.2 配置准备 16
3.7.3 配置策略路由 16
3.7.4 检查配置 17
3.7.5 配置基于 ACL 的策略路由示例 17
4 DHCP 1
4.1 零配置 1
4.1.1 简介 1
4.1.2 配置准备 2
4.1.3 零配置缺省配置 2
4.1.4 配置零配置功能 3
4.1.5 检查配置 3
4.2 DHCP Client 3
4.2.1 简介 3
4.2.2 配置准备 6
4.2.3 配置 DHCP 客户端 7
4.2.4 配置 DHCPv6 客户端 8
4.2.5 检查配置 8
4.2.6 配置 DHCP 客户端示例 8
4.3 DHCP Server 10
4.3.1 简介 10
4.3.2 配置准备 13
4.3.3 创建并配置 IPv4 地址池 13
4.3.4 配置接口的 DHCP Server 功能 14
4.3.5 回收 IP 地址或地址池 14
4.3.6 配置 DHCPv4 Server Ping 功能 14
4.3.7 创建并配置 IPv6 地址池 14
4.3.8 配置接口的 DHCPv6 服务器功能 15
4.3.9 回收 IPv6 地址池 15
4.3.10 检查配置 16
4.3.11 维护 16
4.3.12 配置 DHCPv4 服务器示例 16
4.4 DHCP Relay 18
4.4.1 简介 18
4.4.2 配置准备 19
4.4.3 DHCP Relay 的缺省配置 19
4.4.4 配置接口的 DHCP Relay 功能 19
4.4.5 配置接口的 DHCPv6 Relay 功能 19

4.4.6 配置 DHCP Relay 支持 Option 82 功能 20
4.4.7 配置 DHCPv6 Relay 支持 Option 18/37 功能 20
4.4.8 检查配置 21
4.4.9 维护 21
4.4.10 配置 DHCPv4 中继示例 22
5 QoS 1
5.1 简介 1
5.1.1 服务模型 1
5.2 优先级映射 2
5.2.1 简介 2
5.2.2 配置准备 3
5.2.3 基本 QoS 的缺省配置 4
5.2.4 配置入接口信任的优先级类型 8
5.2.5 配置 DIFFSERV 模版 9
5.2.6 配置出接口 8021P/DSCP 重标记 9
5.2.7 检查配置 10
5.3 队列调度 10
5.3.1 简介 10
5.3.2 配置准备 12
5.3.3 队列调度的缺省配置 12
5.3.4 配置 SP 队列调度 13
5.3.5 配置 WRR 或 SP+WRR 队列调度 13
5.3.6 配置 WFQ 或 SP+WFQ 队列调度 13
5.3.7 配置队列带宽保证 14
5.3.8 检查配置 14
5.3.9 维护 14
5.3.10 配置队列调度示例 15
5.4 拥塞避免 16
5.4.1 简介 16
5.4.2 配置准备 16
5.4.3 拥塞避免的缺省配置 17
5.4.4 配置 WRED 17
5.4.5 检查配置 18
5.5 流量限速 18
5.5.1 简介 18
5.5.2 配置准备 18
5.5.3 配置基于物理接口的流量限速 18
5.5.4 配置基于接口的流量限速示例 19
6 组播 1

6.1 组播概述 1
6.2 IGMP Snooping 6
6.2.1 简介 6
6.2.2 配置准备 6
6.2.3 IGMP Snooping 的缺省配置 7
6.2.4 配置 IGMP Snooping 基本功能 8
6.2.5 配置 IGMP Snooping 查询器功能 8
6.2.6 配置 IGMP Snooping 报文抑制功能 9
6.2.7 配置 IGMP Snooping 组播复制功能 9
6.2.8 配置 IGMP Snooping 静态组播成员功能 9
6.2.9 配置 IGMP Snooping Proxy 功能 10
6.2.10 配置 IGMP Snooping 接口组播组个数限制 10
6.2.11 配置 IGMP Snooping 组播策略 11
6.2.12 配置 IGMP Snooping SSM Mapping 功能 11
6.2.13 配置 IGMP Snooping 静态路由端口配置 12
6.2.14 检查配置 12
6.2.15 维护 12
6.2.16 配置 IGMP Snooping 基本功能应用示例 13
6.2.17 配置 IGMP Snooping 静态成员应用示例 14
6.2.18 配置 IGMP Snooping 组播复制应用示例 16
6.2.19 配置 IGMP Snooping Proxy 应用示例 18
6.2.20 配置 IGMP Snooping 策略应用示例 20
6.3 MLD Snooping 23
6.3.1 简介 23
6.3.2 配置准备 23
6.3.3 MLD Snooping 的缺省配置 24
6.3.4 配置 MLD Snooping 基本功能 24
6.3.5 配置 MLD Snooping 查询器功能 25
6.3.6 配置 MLD Snooping 报文抑制功能 25
6.3.7 配置 MLD Snooping 组播复制功能 26
6.3.8 配置 MLD Snooping 静态组播成员功能 26
6.3.9 配置 MLD Snooping Proxy 功能 26
6.3.10 配置 MLD Snooping 接口组播组个数限制 27
6.3.11 配置 MLD Snooping 组播策略 27
6.3.12 配置 MLD Snooping SSM Mapping 功能 28
6.3.13 检查配置 28
6.3.14 维护 28
6.3.15 配置 MLD Snooping 基本功能应用示例 29
6.3.16 配置 MLD Snooping 静态成员应用示例 30

6.3.17 配置 MLD Snooping 组播复制应用示例 32
6.3.18 配置 MLD Snooping Proxy 应用示例 34
6.3.19 配置 MLD Snooping 策略应用示例 36
7 OAM 1
7.1 简介 1
7.2 EFM 2
7.2.1 简介 2
7.2.2 配置准备 3
7.2.3 缺省配置 3
7.2.4 配置 EFM 基本功能 3
7.2.5 配置 EFM 端口环回功能 4
7.2.6 配置 EFM 链路故障检测功能 5
7.2.7 检查配置 6
7.3 故障转移 6
7.3.1 简介 6
7.3.2 配置准备 6
7.3.3 故障转移功能的缺省配置 7
7.3.4 配置故障转移 7
7.3.5 检查配置 8
7.3.6 配置故障转移示例 8
7.4 VRRP 10
7.4.1 简介 10
7.4.2 配置准备 12
7.4.3 VRRP 的缺省配置 13
7.4.4 配置 VRRP 备份组 13
7.4.5 配置 VRRP6 备份组 15
7.4.6 配置 VRRP 的 Trap 功能 16
7.4.7 配置 VRRP 监视接口 16
7.4.8 配置 BFD for VRRP 17
7.4.9 检查配置 17
7.4.10 配置 VRRP 主备示例 18
7.5 CFM 20
7.5.1 简介 20
7.5.2 配置准备 23
7.5.3 缺省配置 23
7.5.4 配置 CFM 基本功能 23
7.5.5 配置故障检测功能 25
7.5.6 配置故障确认功能 25
7.5.7 配置故障定位功能 26

7.5.8 配置告警抑制功能（仅在 Y1731 模式下可配置） 26
7.5.9 配置单向丢包测试功能（仅在 Y1731 模式下可配置） 27
7.5.10 配置双向时延测试功能（仅在 Y1731 模式下可配置） 27
7.5.11 检查配置 28
7.5.12 配置 CFM 示例 28
8 安全性 1
8.1 ACL 1
8.1.1 简介 1
8.1.2 配置准备 2
8.1.3 配置管理 ACL 2
8.1.4 配置 ACL 3
8.1.5 应用 ACL 8
8.1.6 配置统计 8
8.1.7 配置限速 9
8.1.8 配置时间段 9
8.1.9 检查配置 10
8.1.10 维护 11
8.1.11 配置 ACL 示例 11
8.2 AAA 13
8.2.1 简介 13
8.2.2 配置准备 14
8.2.3 缺省配置 15
8.2.4 配置 RADIUS 服务器 15
8.2.5 配置 TACACS+服务器 16
8.2.6 配置 AAA 服务器组 16
8.2.7 配置 AAA 方法 17
8.2.8 检查配置 17
8.2.9 配置 AAA 示例 18
8.3 802.1x 20
8.3.1 简介 20
8.3.2 配置准备 22
8.3.3 802.1x 功能的缺省配置 22
8.3.4 配置 802.1x 基本功能 23
8.3.5 配置 802.1x 重认证 24
8.3.6 配置 802.1x 定时器 24
8.3.7 检查配置 25
8.3.8 配置 802.1x 示例 25
8.4 安全 MAC 27
8.4.1 简介 27

8.4.2 配置准备 28
8.4.3 安全 MAC 功能的缺省配置 29
8.4.4 配置安全 MAC 基本功能 29
8.4.5 配置接口 Sticky 安全 MAC 地址 30
8.4.6 检查配置 31
8.4.7 维护 31
8.4.8 配置安全 MAC 示例 31
8.5 PPPoE+ 33
8.5.1 简介 33
8.5.2 配置准备 34
8.5.3 PPPoE+功能的缺省配置 35
8.5.4 配置 PPPoE+基本功能 35
8.5.5 配置 PPPoE+报文信息 36
8.5.6 检查配置 38
8.5.7 维护 38
8.5.8 配置 PPPoE+示例 38
8.6 风暴抑制 40
8.6.1 简介 40
8.6.2 配置准备 41
8.6.3 风暴抑制的缺省配置 41
8.6.4 配置风暴抑制功能 41
8.6.5 检查风暴抑制配置 42
8.6.6 配置风暴抑制应用示例 42
8.7 ARP 防攻击 44
8.7.1 配置准备 44
8.7.2 ARP 防攻击缺省配置 44
8.7.3 配置 ARP 防攻击功能 44
8.7.4 检查配置 45
8.7.5 配置 ARP 防攻击示例 46
8.8 ND Snooping 47
8.8.1 简介 47
8.8.2 配置准备 48
8.8.3 ND Snooping 的缺省配置 48
8.8.4 配置 ND Snooping 48
8.8.5 检查配置 49
8.8.6 配置 ND Snooping 示例 49
8.9 DHCP Snooping 51
8.9.1 简介 51
8.9.2 配置准备 52
8.9.3 DHCP Snooping 的缺省配置 52

8.9.4 配置 DHCP Snooping 53
8.9.5 配置 DHCP Snooping 支持 Option 82 功能 54
8.9.6 配置 DHCPv6 Snooping 54
8.9.7 检查配置 55
8.9.8 维护 55
8.9.9 配置 DHCP Snooping 示例 56
8.10 IP Source Guard 57
8.10.1 简介 57
8.10.2 配置准备 58
8.10.3 IP Source Guard 功能的缺省配置 59
8.10.4 配置 IP Source Guard 绑定功能 59
8.10.5 配置 IP Source Guard 接口信任状态 59
8.10.6 检查配置 60
8.10.7 配置 IP Source Guard 示例 60
8.11 CPU 防攻击 61
8.11.1 配置准备 61
8.11.2 配置 CPU 防攻击限速功能 62
8.11.3 检查配置 62
8.11.4 维护 62
8.12 MAC 认证 63
8.12.1 简介 63
8.12.2 缺省配置 63
8.12.3 配置 MAC 认证 64
8.12.4 配置举例 65
8.13 DOS 防攻击 66
8.13.1 简介 66
8.13.2 配置准备 68
8.13.3 DOS 防攻击功能的缺省配置 68
8.13.4 配置畸形报文攻击防范 68
8.13.5 配置分片报文攻击防范 69
8.13.6 配置 TCP SYN 泛洪攻击防范 69
8.13.7 配置 UDP 泛洪攻击防范 69
8.13.8 配置 ICMP 泛洪攻击防范 70
8.13.9 检查配置 70
8.13.10 配置 DOS 防攻击示例 70
9 可靠性 1
9.1 链路聚合 1
9.1.1 简介 1
9.1.2 配置准备 2

9.1.3 缺省配置 2
9.1.4 配置手工链路聚合 3
9.1.5 配置手工主备链路聚合 3
9.1.6 配置静态 LACP 链路聚合 4
9.1.7 配置聚合组负载分担算法 5
9.1.8 检查配置 6
9.1.9 配置静态 LACP 方式的链路聚合示例 7
9.2 G.8031 9
9.2.1 简介 9
9.2.2 配置准备 10
9.2.3 G.8031 的缺省配置 10
9.2.4 创建 G.8031 保护组 10
9.2.5 配置 G.8031 倒换控制 11
9.2.6 检查配置 11
9.2.7 配置 G.8031 保护示例 12
9.3 G.8032 13
9.3.1 简介 13
9.3.2 配置准备 18
9.3.3 G.8032 的缺省配置 18
9.3.4 创建 G.8032 保护环 18
9.3.5 创建 G.8032 保护子环 20
9.3.6 配置 G.8032 倒换控制 21
9.3.7 检查配置 22
9.3.8 维护 22
9.3.9 配置单环 G.8032 保护示例 22
9.3.10 配置相交环 G.8032 保护示例 24
9.4 STP/RSTP 27
9.4.1 简介 27
9.4.2 配置准备 30
9.4.3 STP 的缺省配置 30
9.4.4 使能 STP 功能 31
9.4.5 配置 STP 参数 31
9.4.6 配置 RSTP 边缘接口 32
9.4.7 配置 RSTP 链路类型 32
9.4.8 检查配置 33
9.4.9 配置 STP 示例 33
9.5 MSTP 35
9.5.1 简介 35
9.5.2 配置准备 38
9.5.3 MSTP 的缺省配置 38

9.5.4 使能 MSTP 功能 39
9.5.5 配置 MST 域和 MST 域最大跳数 39
9.5.6 配置设备接口和系统的优先级 40
9.5.7 配置接口的路径开销 41
9.5.8 配置接口最大发送速率 41
9.5.9 配置 MSTP 定时器 42
9.5.10 配置边缘接口 42
9.5.11 配置 BPDU 过滤 43
9.5.12 配置 BPDU 保护 43
9.5.13 配置 STP/RSTP/MSTP 模式切换 44
9.5.14 配置链路类型 45
9.5.15 配置根接口保护 45
9.5.16 配置接口环路保护 45
9.5.17 配置端口 TC 报文抑制功能 46
9.5.18 配置 TC 保护功能 46
9.5.19 检查配置 47
9.5.20 维护 47
9.5.21 配置 MSTP 示例 47
9.6 环路检测 51
9.6.1 简介 51
9.6.2 配置准备 52
9.6.3 环路检测的缺省配置 52
9.6.4 配置环路检测功能 53
9.6.5 检查配置 53
9.6.6 配置环路检测内环应用示例 54
9.7 端口备份 55
9.7.1 简介 55
9.7.2 配置准备 57
9.7.3 接口备份的缺省配置 57
9.7.4 配置接口备份基本功能 58
9.7.5 配置接口强制倒换 59
9.7.6 检查配置 59
9.7.7 配置接口备份示例 59
9.8 端口隔离 61
9.8.1 简介 61
9.8.2 配置准备 62
9.8.3 接口隔离的缺省配置 62
9.8.4 配置接口隔离 62
9.8.5 检查配置 62

9.8.6 配置接口保护示例 63
9.9 L2CP 64
9.9.1 简介 64
9.9.2 配置准备 64
9.9.3 缺省配置 65
9.9.4 配置 L2CP 65
9.9.5 检查配置 66
9.9.6 配置 L2CP 示例 66
9.10 BFD 67
9.10.1 简介 67
9.10.2 配置准备 67
9.10.3 BFD 的缺省配置 67
9.10.4 配置 BFD 单臂回声会话 67
9.10.5 配置 BFD 会话参数 68
9.10.6 检查配置 68
9.10.7 配置 BFD 单跳应用示例 69
9.11 链路震荡保护 70
9.11.1 简介 70
9.11.2 配置准备 70
9.11.3 链路震荡保护的缺省配置 70
9.11.4 配置链路震荡保护 70
9.11.5 检查配置 71
9.11.6 配置链路震荡保护应用示例 71
9.12 接口环回 72
9.12.1 简介 72
9.12.2 配置准备 72
9.12.3 接口环回的缺省配置 72
9.12.4 配置接口环回 72
9.12.5 检查配置 72
9.12.6 配置接口环回应用示例 73
10 系统管理 1
10.1 SNMP 2
10.1.1 简介 2
10.1.2 配置准备 3
10.1.3 SNMP 的缺省配置 4
10.1.4 配置 SNMP v1/v2c 基本功能 4
10.1.5 配置 SNMP v3 基本功能 5
10.1.6 配置 SNMP 其他信息 6
10.1.7 配置 Trap 7

10.1.8 检查配置 8
10.1.9 配置 SNMP v1/v2c 和 Trap 示例 8
10.1.10 配置 SNMP v3 和 Trap 示例 10
10.2 RMON 12
10.2.1 简介 12
10.2.2 配置准备 13
10.2.3 RMON 的缺省配置 13
10.2.4 配置 RMON 统计功能 13
10.2.5 配置 RMON 历史统计功能 14
10.2.6 配置 RMON 告警组 14
10.2.7 配置 RMON 事件组 15
10.2.8 检查配置 15
10.2.9 维护 15
10.2.10 配置 RMON 告警组应用示例 16
10.3 LLDP 17
10.3.1 简介 17
10.3.2 配置准备 20
10.3.3 LLDP 的缺省配置 20
10.3.4 使能全局 LLDP 功能 20
10.3.5 使能接口 LLDP 功能 21
10.3.6 全局配置 LLDP 基本功能 21
10.3.7 接口配置 LLDP 基本功能 22
10.3.8 配置 LLDP 告警功能 22
10.3.9 配置 TLV 23
10.3.10 检查配置 24
10.3.11 维护 24
10.3.12 配置 LLDP 基本功能示例 25
10.4 端口镜像 27
10.4.1 简介 27
10.4.2 配置准备 28
10.4.3 接口镜像的缺省配置 28
10.4.4 配置接口镜像功能 28
10.4.5 VLAN 镜像的缺省配置 29
10.4.6 配置 VLAN 镜像功能 29
10.4.7 检查配置 30
10.4.8 配置接口镜像应用示例 31
10.4.9 配置远端接口镜像应用示例 32
10.5 电缆诊断 33
10.5.1 简介 33

10.5.2 配置准备 33
10.5.3 配置电缆诊断功能 33
10.5.4 检查配置 34
10.6 UDLD 34
10.6.1 简介 34
10.6.2 配置准备 34
10.6.3 UDLD 功能的缺省配置 34
10.6.4 配置 UDLD 35
10.6.5 检查配置 35
10.7 光模块数字诊断 36
10.7.1 简介 36
10.7.2 配置准备 36
10.7.3 光模块数字诊断的缺省配置 37
10.7.4 配置使能光模块数字诊断 37
10.7.5 配置光模块数字诊断告警发送 Trap 37
10.7.6 检查配置 38
10.8 系统日志 38
10.8.1 简介 38
10.8.2 配置准备 39
10.8.3 系统日志的缺省配置 39
10.8.4 配置系统日志基本信息 40
10.8.5 配置系统日志输出 40
10.8.6 配置系统日志输出 TELNET/SSH 终端 41
10.8.7 检查配置 41
10.8.8 维护 42
10.8.9 配置系统日志输出到当前终端示例 42
10.9 告警管理 43
10.9.1 简介 43
10.9.2 配置准备 43
10.9.3 配置告警基本功能 44
10.9.4 检查配置 44
10.10 CPU 监控 45
10.10.1 简介 45
10.10.2 配置准备 45
10.10.3 CPU 监控的缺省配置 45
10.10.4 配置 CPU 监控告警 45
10.10.5 检查配置 46
10.11 内存监控 46
10.11.1 配置准备 46

10.11.2 配置内存监控 47
10.11.3 检查配置 47
10.12 Ping 47
10.12.1 简介 47
10.12.2 配置 Ping 功能 48
10.13 Trace 49
10.13.1 简介 49
10.13.2 配置 IPv4 Trace 功能 49
10.13.3 配置 IPv6 Trace 功能 50
10.14 硬件监控 50
10.14.1 简介 50
10.14.2 温度监控 50
10.14.3 电源监控 51
10.14.4 检查配置 51
10.15 风扇监控 52
10.15.1 简介 52
10.15.2 配置准备 52
10.15.3 配置风扇监控功能 52
10.15.4 检查配置 53
10.16 设备堆叠 53
10.16.1 简介 53
10.16.2 堆叠缺省配置 55
10.16.3 配置堆叠 56
10.16.4 配置举例 57
10.17 MAD 58
10.17.1 简介 58
10.17.2 配置准备 59
10.17.3 配置 MAD 60
10.17.4 配置举例 60
10.18 NQA 61
10.18.1 简介 61
10.18.2 配置准备 62
10.18.3 NQA 的缺省配置 62
10.18.4 配置 ICMP-echo 测试 62
10.18.5 配置 UDP-echo 测试 63
10.18.6 配置 TCP 测试 64
10.18.7 配置 DNS 测试 64
10.18.8 配置 HTTP 测试 65
10.18.9 配置 FTP 测试 66
10.18.10 配置 SNMP 测试 66

10.18.11 配置测试历史记录功能 67
10.18.12 配置测试统计功能 67
10.18.13 配置测试告警功能 68
10.18.14 检查配置 68
10.18.15 维护 68
10.18.16 配置 ICMP-echo 测试功能示例 69
10.19 POE 71
10.19.1 简介 71
10.19.2 配置准备 71
10.19.3 POE 的缺省配置 71
10.19.4 使能 POE 功能 71
10.19.5 配置 POE 最大功率 72
10.19.6 配置 POE 上下电管理 72
10.19.7 配置 PD 描述 73
10.19.8 检查配置 73
10.19.9 维护 73
10.19.10 配置 POE 示例 73
10.20 U 盘部署 75
10.20.1 简介 75
10.20.2 U 盘部署流程 75
10.20.3 配置准备 76
10.20.4 U 盘部署的缺省配置 76
10.20.5 制作快速部署 U 盘 77
10.21 PATCH 补丁功能 78
10.21.1 简介 78
10.21.2 配置准备 78
10.21.3 加载补丁 78
10.21.4 激活补丁 78
10.21.5 去激活补丁 78
10.21.6 删除补丁 79
10.21.7 维护 79
10.21.8 PATCH 示例 79
10.22 定时备份配置功能 80
10.22.1 简介 80
10.22.2 配置准备 80
10.22.3 配置 timerange 80
10.22.4 配置自动上传 81
10.22.5 检查配置 82
10.22.6 定时备份配置示例 82

11 附录 1
11.1 术语 1
11.2 缩略语 5

图目录

图 1-1 通过 PC 连接 Console 口登录设备的组网示意图 3
图 1-2 “超级终端”中的通信参数配置示意图 3
图 1-3 交换机作为 Telnet Server 设备的组网示意图 5
图 1-4 交换机设备作为 Telnet Client 设备的组网示意图 5
图 1-5 NTP 基本原理 18
图 1-6 NTP 组网示意图 22
图 2-1 MAC 地址表转发示意图 2
图 2-2 MAC 应用组网示意图 8
图 2-3 VLAN 划分示意图 9
图 2-4 VLAN 和接口保护组网示意图 17
图 2-5 IP 电话单独接入交换机组网示意图 20
图 2-6 基本 QinQ 典型组网示意图 25
图 2-7 基本 QinQ 应用组网示意图 29
图 2-8 灵活 QinQ 应用组网示意图 30
图 2-9 VLAN 转换原理组网示意图 32
图 2-10 VLAN 转换应用组网示意图 34
图 2-11 MVRP 原理示意图 37
图 2-12 MVRP 应用组网示意图 39
图 3-1 配置 VLAN 接口组网示意图 3
图 3-2 配置 ARP 组网示意图 9
图 3-3 NDP 地址解析原理示意图 10
图 3-4 配置静态路由组网示意图 14
图 3-5 配置策略路由组网示意图 17
图 4-1 零配置服务器组网示意图 2
图 4-2 DHCP 典型应用组网示意图 4

图 4-3 DHCP 报文结构示意图 4
图 4-4 DHCP 客户端组网示意图 6
图 4-5 配置 DHCP 客户端组网示意图 9
图 4-6 DHCP Server 和 DHCP Client 应用组网示意图 11
图 4-7 DHCP 报文结构示意图 11
图 4-8 配置 DHCP 服务器组网示意图 17
图 4-9 DHCP Relay 工作原理示意图 18
图 4-10 配置 DHCP 中继组网示意图 22
图 5-1 SP 调度示意图 11
图 5-2 WRR 调度示意图 11
图 5-3 WFQ 调度示意图 12
图 5-4 配置队列调度组网示意图 15
图 5-5 配置基于接口的流量限速组网示意图 19
图 6-1 组播方式传输信息示意图 2
图 6-2 组播基本概念在网络中相应位置标示示意图 3
图 6-3 IPv4 组播地址和组播 MAC 地址的映射关系 4
图 6-4 IGMP 和二层组播特性运行位置示意图 5
图 6-5 IGMP Snooping 应用场景 7
图 6-6 IGMP Snooping 基本功能组网应用示意图 13
图 6-7 IGMP Snooping 静态成员功能组网应用示意图 15
图 6-8 IGMP Snooping 组播复制功能组网应用示意图 17
图 6-9 IGMP Snooping Proxy 功能组网应用示意图 19
图 6-10 IGMP Snooping 组播策略功能组网应用示意图 21
图 6-11 MLD Snooping 应用场景 23
图 6-12 MLD Snooping 基本功能组网应用示意图 29
图 6-13 MLD Snooping 静态成员功能组网应用示意图 31
图 6-14 MLD Snooping 组播复制功能组网应用示意图 33
图 6-15 MLD Snooping Proxy 功能组网应用示意图 35
图 6-16 MLD Snooping 组播策略功能组网应用示意图 37
图 7-1 OAM 环回示意图 2
图 7-2 故障转移应用组网示意图 9
图 7-3 VRRP 原理示意图 11

图 7-4 VRRP 负载分担原理示意图 12
图 7-5 配置 VRRP 主备组网图 18
图 7-6 不同级别 MD 网络示意图 21
图 7-7 不同级别 MD 网络示意图 21
图 7-8 CFM 典型配置组网图 29
图 8-1 ACL 示例 11
图 8-2 分域认证应用组网示意图 18
图 8-3 802.1x 认证体系结构 20
图 8-4 802.1x 应用组网示意图 26
图 8-5 安全 MAC 应用组网示意图 32
图 8-6 用户通过 PPPoE 认证连接网络示意图 34
图 8-7 PPPoE+应用组网示意图 39
图 8-8 风暴抑制应用组网示意图 43
图 8-9 动态 ARP 检测应用组网示意图 46
图 8-10 配置 ND Snooping 组网示意图 50
图 8-11 DHCP Snooping 组网示意图 51
图 8-12 配置 DHCP Snooping 组网示意图 56
图 8-13 IP Source Guard 功能示意图 58
图 8-14 IP Source Guard 应用组网示意图 60
图 8-15 MAC 认证组网示意图 65
图 8-16 DOS 防攻击应用组网示意图 71
图 9-1 静态 LACP 方式链路聚合应用组网示意图 7
图 9-2 G.8031 组网示意图 12
图 9-3 G.8032 环网示意图 14
图 9-4 环网空闲状态 15
图 9-5 环网保护状态 16
图 9-6 子环模型 17
图 9-7 单环 G.8032 应用组网示意图 23
图 9-8 相交环 G.8032 应用组网示意图 25
图 9-9 网络环路造成网络风暴示意图 28
图 9-10 运行 STP 协议的环网示意图 29
图 9-11 RSTP 协议造成 VLAN 报文无法转发示意图 30

图 9-12 STP 应用组网示意图 33
图 9-13 MSTP 网络基本概念示意图 36
图 9-14 MSTI 概念示意图 37
图 9-15 MST 域内多生成树实例组网示意图 38
图 9-16 MSTP 应用组网示意图 48
图 9-17 环路类型示意图 51
图 9-18 环路检测内环应用组网示意图 54
图 9-19 接口备份原理示意图 56
图 9-20 接口备份在不同 VLAN 上的应用原理示意图 57
图 9-21 接口备份应用组网示意图 60
图 9-22 接口保护组网示意图 63
图 9-23 L2CP 拓扑图 64
图 9-24 BFD 单跳应用 69
图 10-1 SNMP 工作机制示意图 2
图 10-2 SNMP v3 认证机制示意图 5
图 10-3 SNMP v1/v2c 组网示意图 9
图 10-4 SNMP v3 和 Trap 组网示意图 10
图 10-5 RMON 应用示意图 12
图 10-6 RMON 典型应用组网示意图 16
图 10-7 LLDPDU 结构图 18
图 10-8 基本 TLV 结构图 18
图 10-9 配置 LLDP 基本功能组网示意图 25
图 10-10 接口镜像功能原理示意图 27
图 10-11 接口镜像应用组网示意图 31
图 10-12 接口远端镜像应用组网示意图 32
图 10-13 系统日志输出到日志主机组网示意图 42
图 10-14 Ping 功能实现原理组网示意图 48
图 10-15 Trace 功能实现原理组网示意图 49
图 10-16 2 台成员设备组成链型拓扑 55
图 10-17 2 台成员设备组成环形型拓扑 55
图 10-18 2 台堆叠拓扑图 57
图 10-19 MAD 直连模式 59

图 10-20 MAD 代理模式 59
图 10-21 配置 ICMP-echo 测试功能组网示意图 69
图 10-22 U 盘快速部署流程示意图 76

表格目录

表 2-1 接口模式与报文转发 10
表 4-1 DHCP 报文字段含义列表 5
表 4-2 DHCP 报文字段含义列表 11
表 5-1 缺省情况下 8021p 入方向和本地优先级及颜色的映射关系 4
表 5-2 缺省情况下 8021p 出方向和本地优先级及颜色的映射关系 4
表 5-3 缺省情况下 DSCP 入方向和本地优先级及颜色的映射关系 5
表 5-4 缺省情况下 DSCP 出方向和本地优先级及颜色的映射关系 7
表 10-1 TLV 类型 18
表 10-2 IEEE 802.1 组织定义的 TLV 19
表 10-3 IEEE 802.3 组织定义的 TLV 19
表 10-4 信息级别 39

1 基础配置

本章介绍交换机设备的基础配置信息及配置过程，并提供相关的配置案例。

- 登录设备
- 加载与升级
- 时间管理
- PTP
- 接口管理

1.1 登录设备

1.1.1 简介

登录交换机设备进行配置和管理，可以采用 CLI（Command-Line Interface，命令行界面）方式、Web 方式。

交换机命令行方式下有多种配置方式：

- Console 方式：第一次配置时必须采用 Console 方式，甲信设备支持 RJ45、M12、Micro USB 和 Mini-USB 类型的 Console 口。
- Telnet 方式：设备默认 IP 地址为 192.168.0.1。如需修改 IP 地址，需要先通过 Console 方式登录，在设备上配置 IP 地址，以及设置用户名和密码，再使用新 IP 地址进行远程 Telnet 配置。
- SSH 方式：在通过 SSH 登录设备之前，需要先通过 Console 接口登录设备并启动 SSH 服务。

当需要在 Web 方式下配置时，也必须先通过命令行方式，配置 VLAN 接口 IP 地址，然后才可以通过 NView NNM 网管平台对设备进行配置。

1.1.2 通过 Console 口登录设备

说明

- 设备均支持 RJ45 类型的 Console 口。
- 设备使用黑色线序 Console 线缆，如不确定，请查看该设备系列对应的《用户手册》或《产品描述》手册，或咨询我司技术人员。
- 以下均以 RJ45 类型 Console 口为例进行说明。

简介

Console 口是网络设备用来与运行终端仿真程序的 PC 进行连接的常用接口，用户可以借助此接口对本地设备进行配置和管理。这种管理方式不需借助网络进行通信，所以被称为带外（out-of-band）管理方式，在网络运行异常的情况下，用户也可以通过 Console 口对设备进行配置和管理。

在以下两种情况中，只能通过 Console 口登录设备进行配置：

- 设备第一次加电启动
- 无法通过 Telnet 方式登录设备

缺省配置

设备上 Console 口的缺省配置如下。

功能	缺省值
传输速率	115200
流控方式	无流控
验证方式	不验证
停止位	1
数据位	8

通过 Console 口登录

当用户希望通过 PC 连接 Console 口登录设备时，首先需要通过配置线缆将设备的 Console 口和 PC 的 RS-232 串口相连，如图 1-1 所示，然后在 PC 上运行终端仿真程序，如微软公司的 Windows XP 操作系统自带的“超级终端”程序，将通信参数如图 1-2 配置，完成后即可登录设备。

图 1-1 通过 PC 连接 Console 口登录设备的组网示意图

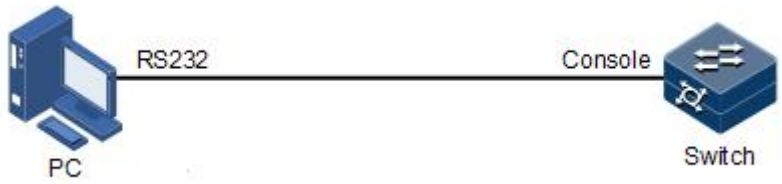


图 1-2 “超级终端”中的通信参数配置示意图

说明

初始情况下串口波特率为 115200。

配置 Console 口

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure** JX(config)#**line console** JX(config-line-console)#**baudrate { 115200 | 9600 }**	修改串口登录波特率。

配置 Console 密码和认证方式

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure** JX(config)#**line console password**	设置串口密码。
2	JX(config)#**line console** JX(config-line-console)#**login authentication { aaa | local | password | none }**	设置串口认证方式 • local：用户名密码 • password：串口密码 • none：不认证

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show line console information**	查看串口波特率配置信息。

1.1.3 通过 Telnet 登录设备

简介

说明

初始情况下，设备缺省管理 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0。如需修改设备 IP 地址，用户可以通过 Console 口登录设备，并对设备进行配置。设备的缺省用户名和密码均为 JX。Telnet 连接状态下输错 3 次密码自动断开连接。

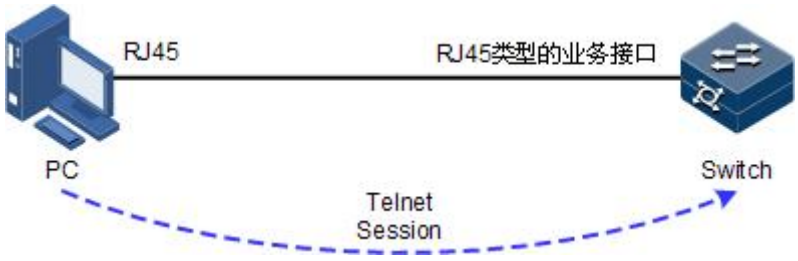
Telnet 提供了一种通过 PC 远程登录设备的方式。用户可以先通过 PC 登录到一台网络设备，然后再通过 Telnet 方式远程登录到联网的其他网络设备，而不需要为每一台网络设备都连接一台 PC。

有 SNMP 接口的设备，需使用 SNMP 接口进行 telnet 登录。无 SNMP 接口的设备，可以使用任意接口进入管理 VLAN 进行 telnet 登录。

交换机设备提供的 Telnet 服务包括：

- Telnet Server：用户在 PC 上运行 Telnet 客户端程序登录到设备，对设备进行配置管理。如下图所示，交换机此时提供的是 Telnet Server 服务。

图 1-3 交换机作为 Telnet Server 设备的组网示意图

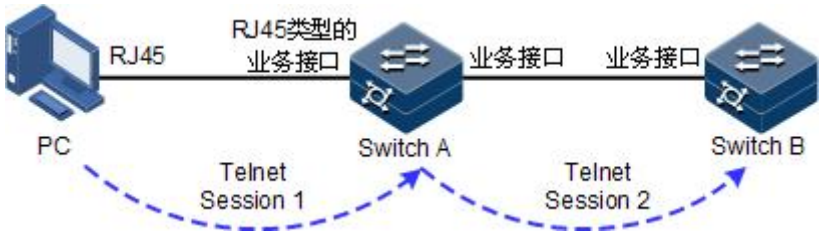


说明

设备支持 Telnet 最大用户数为 10 个。

- Telnet Client：用户在 PC 上通过终端仿真程序或 Telnet 客户端程序建立与设备的连接后，再通过 telnet 命令登录到其它设备，对其进行配置管理。如下图所示，Switch A 此时既作为 Telnet Server，也同时提供 Telnet Client 服务。

图 1-4 交换机设备作为 Telnet Client 设备的组网示意图



缺省配置

设备上 Telnet 服务器功能的缺省配置如下。

功能	缺省值
Telnet 服务器功能状态	使能
Telnet 服务器监听端口号	23
使能 Telnet 服务器功能的接口	所有接口

功能	缺省值
最大 Telnet 连接数	10

通过 Telnet 配置设备时，建议不要频繁修改设备的 IP 地址。修改 IP 地址可能导致当前 Telnet 连接断开，需根据新的 IP 地址重新建立 Telnet 连接。

配置 Telnet 服务器

在通过 Telnet 登录设备之前，用户需要通过 Console 接口登录设备并启动 Telnet 服务，请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id* JX(config)#**interface ge 1/0/1**	进入 VLAN 接口或带外接口配置模式，以下使用进入 VLAN 接口为例。
3	JX(config-vlan*)#**ip address** *ip-address* [*ip-mask*] [**sub**] JX(config-vlan*)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**] JX(config-vlan*)#**exit**	配置设备 IP 地址。
4	JX(config)#**telnet server start**	开启设备 Telnet Server 功能。
5	JX(config)#**telnet server stop**	断开指定的 Telnet 连接。
6	JX(config)#**telnet server start**	开启设备 IPv4 Telnet Server 功能。
7	JX(config)#**telnet-ipv6 server stop**	断开指定的 IPv6 Telnet 连接。

配置 Telnet 服务器端口号

Telnet 缺省端口号为 23，可进行以下配置修改端口号。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**telnet server port** {*port-number* | **default**}	修改 Telnet IPv4 服务端口号。
3	JX(config)#**telnet-ipv6 server start**	开启设备 IPv6 Telnet Server 功能。

步骤	配置	说明
4	JX(config)#**telnet-ipv6 server port** {*port-number* | **default**}	修改 Telnet IPv6 服务端口号。

配置 Telnet 客户端

请在作为 Telnet Client 的设备上进行以下配置。

步骤	配置	说明
1	JX#**telnet** *ipv4-address* [**-p** *port-id* | **-s** *source-ipv4-address*]* JX#**telnet-ipv6** *ipv6-address* [**-p** *port-id* | **-s** *source-ipv6-address*]*	以 Telnet 方式登录其他设备。

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show running-config**	查看 Telnet Server 的配置情况。

1.1.4 通过 SSH 登录设备

简介

Telnet 缺少安全的认证方式，而且传输过程采用 TCP（Transmission Control Protocol，传输控制协议）进行明文传输，存在很大的安全隐患。单纯提供 Telnet 服务容易招致 DoS（Deny of Service，拒绝服务）、主机 IP 地址欺骗、路由欺骗等恶意攻击。

传统的 Telnet 和 FTP（File Transfer Protocol，文件传输协议）通过明文传送密码和数据的方式，已经慢慢不被用户所接受。SSH 是一个网络安全协议，通过对网络数据的加密，可以有效防止远程管理过程中的信息泄露问题，在网络环境中为远程登录和其他网络服务提供了更高的安全性。

SSH 通过 TCP 进行数据交互，它在 TCP 之上构建了一个安全的通道。另外，SSH 服务除了支持标准端口 22 以外，还支持其他服务端口，以防止设备受到来自网络的非法攻击。

在通过 SSH 登录设备之前，用户需要通过 Console 接口登录设备并启动 SSH 服务。

设备支持基于密码和公钥两种认证方式。

- 基于密码认证方式：与登录设备认证使用同一数据库。SSH 客户端只需输入用户名和密码，就可以登录到远程 SSHv2 服务器。所有传输的数据都会被加密，但是可能会有其他服务器伪冒真正的服务器，无法避免伪冒服务器攻击。

- 基于公钥认证方式：SSHv2 客户端除需要输入用户名和密码外，还需要依靠密钥进行认证。登录前在 SSHv2 客户端创建一对密钥，包括主机公钥和主机私钥，并将公钥存入 SSHv2 服务器。登录认证过程和传输的数据都会被加密，避免了伪冒服务器攻击。

缺省配置

设备上 SSH 登录设备的缺省配置如下。

功能	缺省值
SSH 服务器功能状态	禁止
本地 SSH 密钥对长度	512bit
密钥重协商周期	0h
SSH 采用的认证方式	password
SSH 认证超时时间	600s
SSH 侦听端口号	22
SSH 会话功能状态	禁用
SSH 协议版本	v2
SSH 安全算法模式	禁止

配置 SSH 服务器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**ssh server start**	开启设备 IPv4 SSH Server 功能
3	JX(config)#**ssh server stop**	关闭设备 IPv4 SSH Server 功能
2	JX(config)#**ssh-ipv6 server start**	开启设备 IPv4 SSH Server 功能
3	JX(config)#**ssh-ipv6 server stop**	关闭设备 IPv6 SSH Server 功能

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show ssh config**	查看 SSH 配置信息。

1.1.5 通过 Web 登录设备

简介

为了方便用户对设备进行配置和维护，设备支持 Web 网管功能。用户可以利用 Web 网管在图形界面下直观的管理和配置设备。

Web 网管支持以下两种文本传输协议：

- HTTP（Hypertext Transfer Protocol，超文本传输协议）：用来在网络上传递 Web 页面信息。在设备上使能 HTTP 服务功能后，用户就可以通过 HTTP 协议登录设备，并利用 Web 界面访问、控制设备。
- HTTPS（Secure Hypertext Transfer Protocol，安全的超文本传输协议）：利用 SSL（Secure Sockets Layer，安全套接层）协议保证合法客户端可以安全访问设备。客户端与设备之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现对设备的安全管理。

配置 Web 网管功能后，远程用户可以通过 Web 浏览器登录设备并对其进行管理。如果禁止 Web 网管功能，则断开所有已经建立的 HTTP 连接。

缺省配置

设备上 Web 网管的缺省配置如下。

功能	缺省值
HTTP 功能状态	使能

配置 Web 网管功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**http server { start | stop }**	使能 HTTP 功能，使用 **stop** 格式禁止该功能。
3	JX(config)#**https server { start | stop }**	使能 HTTPS 功能，使用 **stop** 格式禁止该功能。

检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show running-config**	查看设备配置信息。

1.1.6 管理登录用户

简介

第一次启动交换机设备时，用户只要将 PC 通过 Console 接口与设备连接，在超级终端中输入初始的用户名和密码，即可以登录设备并对其进行配置。

说明

初始情况下，设备的用户名为 JX，密码为 JX。

如果为设备的业务接口配置了 IP 地址，在没有任何权限控制的情况下，任意远端用户都可以通过 Telnet 方式登录设备，或者通过与设备建立 PPP（Point to Point Protocol，点对点协议）连接来访问网络，这显然对设备和网络都是不安全的。为此需要为设备创建用户并设置密码和权限，对登录用户进行管理。

缺省配置

设备上用户管理的缺省配置如下。

功能	缺省值
本地用户信息	• 用户名：JX • 密码：JX • 用户权限：15
新建用户权限	15
新建用户激活状态	**active**
新建用户服务类型	console、telnet、ssh、ftp、http
密码复杂度	**3**
用户名复杂度	**1**
用户名最大长度	**64**
密码最大长度	**64**
缺省支持特殊字符	`~!@#$%^&*()_-+={}[]|\:;'<>",./

配置本地用户管理

请在设备上进行以下配置。

步骤	配置	说明
1	JX(config)#**username** *user-name* **password** { **cipher** | **reversible-cipher** | **plain** } *password* **group { administrators** | **operators** | **users** | **guests** } **domain** [**telnet** | **ssh** | **http** | **ftp** | **console** | **default** | **all**]]*	创建或修改登录用户的用户名和密文形式密码。
2	JX(config)#**username** *user-name* **domain** [**telnet** | **ssh** | **http** | **ftp** | **console** | **default** | **all**]*	修改用户组域。
3	JX(config)#**username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** }	修改用户组。
4	JX(config)#**user password-complex** { *complex* | **default** }	配置用户密码复杂度，默认值为 3。
4	JX(config)#**user password-length** { *length* | **default** }	配置用户密码最小长度，默认值为 8。
5	JX(config)#**user name-complex** { *complex* | **default** }	配置用户名复杂度，默认值为 1。
6	JX(config)#**user name-length** { *length* | **default** }	配置用户名长度，默认值为 1。
7	JX(config)#**username** *user-name* **{ login-lock | manual-lock | unlock } [reauth-interval** { *interval* **| default** } | **fail-count** { *count* **| default]***	配置用户锁定类型为 登录锁定（login-lock）时可以配置登录失败次数和重认证间隔。
8	JX#**show user name** *user-name*	查看配置用户的信息
9	JX#**user special-characters** *CHARLIST*	配置用户名称和用户密码可包含的特殊字符

说明

- 除缺省用户外，设备最多可再创建 30 个本地用户。
- 用户启用登录锁定（login-lock）时可配置最大登录失败次数和重认证间隔，默认失败次数上限是 3 次，重认证时间间隔为 10s。当登录失败达上限并且在静默时间内设备处于登录锁定，此时无法登录。超过静默时间，解除锁定，也可通过 unlock 手动解除锁定。
- 用户启动手工锁定（manual-lock）将会一直锁定，不受失败次数和重认证间隔限制。可通过 unlock 手动解除锁定

1.1.7 用户密码恢复

简介

当用户忘记设备登录用户密码时，用户只要将 PC 通过 Console 接口与设备连接，在超级终端中进入临时密码视图，获取临时密码序列号，可通过临时密码序列号生成临时密码。临时密码校验成功登录设备后，需要用户再次修改本地用户的密码。

说明

密码恢复操作只能在 Console 终端进行。在登录界面输入快捷键“CTRL+P”进入临时密码视图。

临时密码恢复功能缺省开启状态。

配置临时密码恢复

请在设备上进行以下配置。

步骤	配置	说明
1	快捷键 CTRL+P	在 Console 登录界面键入快捷键
2	JX(key)#**get temporary-password-serial**	获取临时密码序列号
3	JX(key)#**check temporary-password** *password*	校验临时密码
4	JX(config)#**temporary-password** { enable | disable }	开启关闭临时密码恢复功能。

1.1.8 终端属性设置

简介

用户可以设置 Console，Telnet，SSH 终端的超时时间，屏幕逐页滚动控制，终端颜色，大小写敏感，交互模式等终端属性。

配置终端属性

请在设备上进行以下配置。

步骤	配置	说明
1	JX(config)#**terminal length** { 0 | *length* | default }	设置屏幕逐页滚动的条数。 0：不逐页滚动，直接全部输出 缺省逐页滚动为 24 行
2	JX(config)#**terminal timeout** { 0 | *timeout* }	设置终端超时时间。 0：终端不超时 缺省超时时间 10 分钟
3	JX(config)#**terminal monitor** JX(config)#**no terminal monitor**	开启关闭终端信息监控
4	JX(config)#**terminal mmi-mode** { enable | disable }	开启关闭设备人机交互模式。
5	JX(config)#**case-sensitive** { enable | disable }	开启关闭输入大小写字母敏感功能

1.1.9 Bootrom 密码设置

简介

用户可以设置 bootrom 密码。

配置终端属性

请在设备上进行以下配置。

步骤	配置	说明
1	JX(config)#**bootrom password** *PASSWORD*	设置 bootrom 密码
2	JX(config)#**no bootrom password**	清除 bootrom 密码
3	JX(config)#**show bootrom password**	查看 bootrom 密码

1.1.10 登录方式修改（弱口令漏洞解决方案）

简介

为解决弱口令漏洞问题，设备从 v7.01.50 版本开始，修改了登录方式：

- 缺省为串口密码方式登录，无缺省用户；
- telnet 和 web(ssh 不支持)首次登录可配置用户。

串口登录

缺省为串口密码登录，启动后提示是否配置串口密码：

```
INFO: the console password is empty.For security purpose,please set
password,Yes?(y/n):
```

- 选择“n”：暂不配置密码，直接进入系统。下次重启后，会再次提示；
- 选择“y”：需配置串口密码，该密码自动保存。后续登录，则需要验证密码；

Telent/Web 登录

缺省无用户，若需要远程登录（telnet/web/ssh），则需要先创建用户。

- 可通过串口登录，然后创建用户；
- telnet/web 首次登录，可直接创建用户；

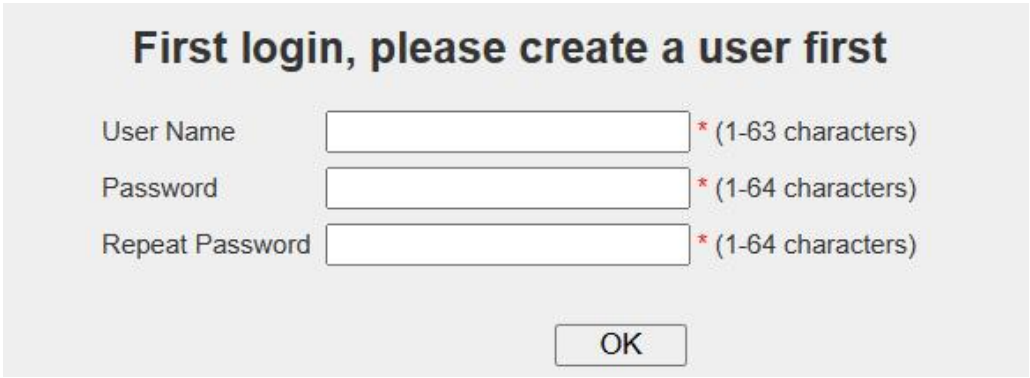
说明

首次登录，是指设备无启动配置，且通过带外口及带外缺省 IP 连接设备。

telnet 登录

```
INFO: The device has no user,please create a new user now.
     new password length must be 8-64 characters,password complexity must
be at least 3 classes(eg.uppercase,lowercase,digits,other special
characters...)
New Username:
```

web 登录



1.2 加载与升级

1.2.1 简介

加载

传统的配置文件加载方式为串口加载，该方式加载速度慢、耗时长、不具备远程加载功能，导致操作很不方便。为了解决这些问题，引入了 FTP 加载方式、TFTP 加载方式等。

设备提供多种方法用于确定设备在 TFTP/FTP 服务器上的配置文件名称，比如手动输入、使用 DHCP 客户端获取、使用默认的配置文件名。除此之外，用户还可以指定某种配置文件命名规则，根据规则使用设备自身的属性（例如设备型号、MAC 地址、软件版本号）确定与指定设备对应的配置文件名称。

升级

当需要为设备增加新特性、优化原有功能或解决当前软件版本的 BUG 时，可以对设备进行升级。

设备支持以下升级方式：

- 命令行升级方式

1.2.2 通过 TFTP 命令行升级方式升级系统软件

在通过命令行升级方式升级系统软件前，需要首先搭建 TFTP 环境，PC 作为 TFTP 服务器，交换机设备作为客户端，基本要求如下：

- 将 TFTP 服务器网口和交换机接口用网线连接，交换机设备默认 IP 地址为 192.168.0.1。
- 配置 TFTP 服务器端，确保服务器处于可用状态。
- 配置 TFTP 服务器的 IP 地址，使之与设备的 IP 地址处于同一网段，使设备可以访问服务器。

通过命令行升级方式升级系统软件的步骤如下：

步骤	配置	说明
1	JX#{**tftp | tftp-ipv6 } get** {*ipv4-address | ipv6-address* } *remote-file-name* [**localfile** *local-file-name*]	通过 TFTP 协议下载系统启动软件。支持 IPv6 地址。
2	JX#**upgrade os [localfile** *local-file-name*]	升级系统软件。
3	JX#**reboot**	重新启动设备。

1.2.3 通过 FTP 命令行升级方式升级系统软件

在通过命令行升级方式升级系统软件前，需要首先搭建 FTP 环境，PC 作为 FTP 服务器，交换机设备作为客户端，基本要求如下：

- 将 FTP 服务器网口和交换机接口用网线连接，交换机设备默认 IP 地址为 192.168.0.1。
- 配置 FTP 服务器端，确保服务器处于可用状态。
- 配置 FTP 服务器的 IP 地址，使之与设备的 IP 地址处于同一网段，使设备可以访问服务器。

通过命令行升级方式升级系统软件的步骤如下：

步骤	配置	说明
1	JX#{**ftp | ftp-ipv6 } get** {*ipv4-address | ipv6-address* } *user-name user-password remote-file-name* [**localfile** *local-file-name*]	通过 FTP 协议下载系统启动软件。支持 IPv6 地址。
2	JX#**upgrade os [localfile** *local-file-name***]**	升级系统软件。
3	JX#**reboot**	重新启动设备。

1.2.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show startup-config**	查看设备启动时加载的配置信息。
2	JX#**show running-config**	查看设备的当前配置信息。
3	JX#**show version**	查看系统的版本信息。

1.2.5 指定系统启动镜像

指定启动镜像为主或备镜像，请在设备上执行以下命令。

序号	检查项	说明
1	JX(config)#**boot os {main | backup}**	指定系统启动镜像为主或备镜像，设置完成后下一次启动生效。仅设备支持双镜像时可选择，缺省系统从主镜像启动。

1.2.6 检查系统版本信息

查看系统版本信息，请在设备上执行以下命令查看结果。

序号	检查项	说明
1	JX#show os-package	查看系统版本信息，包括主备镜像版本信息、版本大小、编译时间等。

1.3 时间管理

1.3.1 简介

随着互联网在社会各个方面的发展和延伸，网络上多种涉及时间的应用，如网上实时交易、分布性的网络计算和处理、交通航班航路管理、数据库管理等，都需要精确、可靠的时间。

为了保证设备系统时间的精准，设备提供了完善的时间管理功能，包括手动配置系统时间和时区、手动配置夏令时、NTP 功能以及 SNTP 功能。

时间和时区

通常情况下设备时间配置为设备所在地的实时时间，将时区配置为以格林尼治标准时间为基础的所在地时区（如中国北京在格林尼治为基准的东八区，即配置为+08:00）。

设备支持“年月日时分秒”的时间显示和时区偏移显示，可手动配置设备的时间和时区。

夏令时

夏令时（DST，Daylight Saving Time）是一种为节约资源而人为规定地方时间的制度。一般在夏季人为将时间调整提前一小时，可以使人早起早睡以减少照明量。但各个国家对夏令时的具体规定不同，所以在配置夏令时前需要考虑当地的具体情况。

设备支持配置夏令时开始的时间和结束的时间，以及调整时间的偏移量。

NTP

NTP（Network Time Protocol，网络时间协议）是用于互联网中时间同步的标准互联网协议，用于快速使网络内所有具有时钟的设备进行时钟同步。NTP 基于 UDP 进行传输，使用的端口号是 123，保证较高的精度（误差在 10ms 左右）。

NTP 基本原理如下图所示，时钟同步的工作过程如下：

步骤 1 Switch A 发送一个 NTP 消息包给 Switch B，该消息包带有离开 Switch A 时的时间戳，该时间戳为 10:00:00am，记为 t1。

步骤 2 当此 NTP 消息包到达 Switch B 时，Switch B 加上自己的时间戳，该时间戳为 11:00:01am，记为 t2。

步骤 3 当此 NTP 消息包离开 Switch B 时，Switch B 再加上自己的时间戳，该时间戳为 11:00:02am，记为 t3。

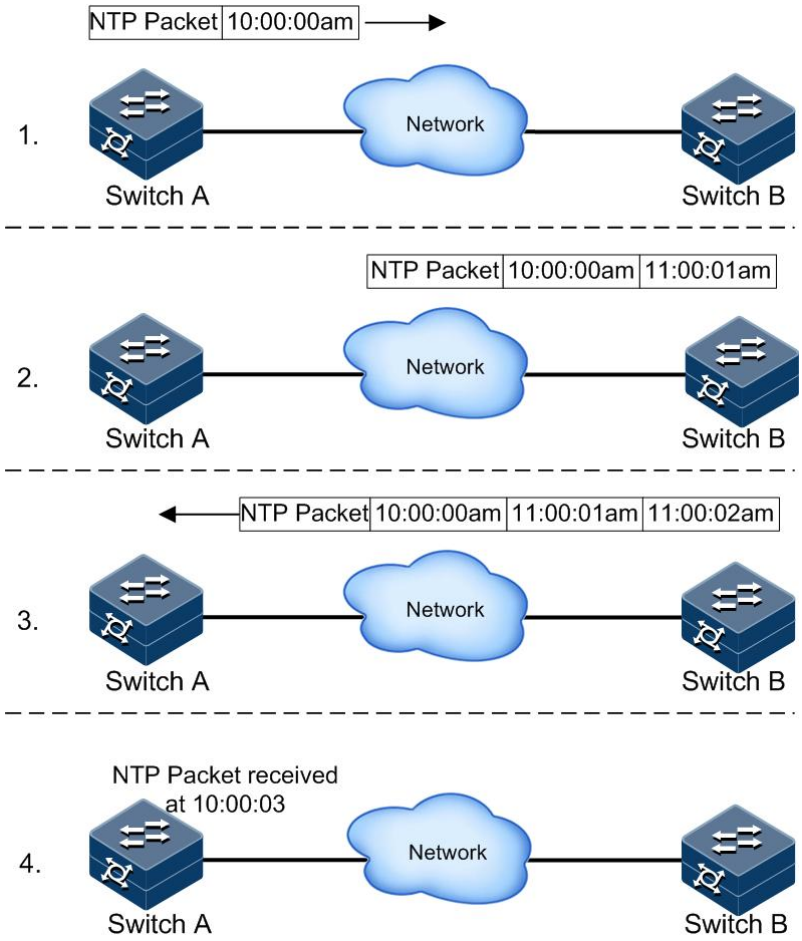
步骤 4 当 Switch A 接收到该响应消息包时，加上一个新的时间戳，该时间戳为 10:00:03am，记为 t4。

至此，Switch A 已经拥有足够的信息来计算两个重要的参数：

- NTP 消息来回一个周期的时延：Delay=(t4-t1)-(t3-t2)。
- Switch A 和 Switch B 之间的时间差：Offset=((t2-t1)+(t3-t4))/2。

Switch A 根据这些信息来设定自己的时钟，实现与 Switch B 的时钟同步。

图 1-5 NTP 基本原理



NTP 支持多种工作模式进行时间同步：

- 服务器/客户端模式

在服务器/客户端模式中，客户端向不同的服务器发送时钟同步报文。服务器收到报文后会发送应答报文。客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器。

在该模式下，客户端仅能同步服务器的时间，而服务器无法同步客户端的时间。设备不能既作为客户端又作为服务器。

- 对等体模式

在对等体模式中，配置对等体的设备可以向层级高的设备或者服务器进行对时。

已配置 NTP 服务器的设备不能再配置对等体。

SNTP

SNTP（Simple Network Time Protocol，简单网络时间协议）将设备系统时间同步为格林尼治时间，然后根据系统时区的设置来转化成本地时间。当 SNTP 客户端与服务器不在同一地区时，SNTP 客户端同步的时间为格林威治时间，然后根据系统时区的设置来转化成本地时间。

SNTP 客户端获取时间有两种方式，即主动发送请求报文和被动监听报文，通过不同模式实现：

- 单播模式：SNTP 客户端主动发送请求报文。指定设备的 SNTP 单播服务器地址后，设备将每隔 10s 尝试一次从 SNTP 服务器获取时钟信息，并且每次从 SNTP 服务器获取时钟信息的最大超时时间为 3 秒。
- 组播或广播模式：SNTP 客户端被动监听报文。
  - 配置 SNTP 客户端为组播模式后，设备将时刻监听组播地址 224.0.1.1，从 SNTP 组播服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为服务器发送周期的 1.5 倍。
  - 配置 SNTP 客户端为广播模式后，设备将时刻监听广播地址 255.255.255.255，从 SNTP 广播服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为服务器发送周期的 1.5 倍。

1.3.2 配置准备

场景

配置设备的系统时间，保证系统时间的精准。

- 无论何时，手动配置时间和时区立即生效。
- 开启 NTP 或 SNTP 功能，经过同步周期后，设备同步到的时间会实时刷新，覆盖当前系统时间。
- NTP 功能与 SNTP 功能互斥，不能同时配置。

前提

无

1.3.3 缺省配置

NTP

设备上 NTP 的缺省配置如下。

功能	缺省值
设备是否作为 NTP 主时钟	否

功能	缺省值
全局 NTP 服务器	无
全局 NTP 对等体	无
参考时钟源	0.0.0.0
身份验证功能	关闭
身份验证密钥 ID	无
可信密钥	无

SNTP

设备上 SNTP 的缺省配置如下。

功能	缺省值
SNTP 服务器地址	无

1.3.4 配置 NTP

配置 NTP 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**ntp client update-interval** { *interval* | **default** }	配置 ntp client 通告时间 interval：通告间隔时间，范围 3～17 秒 缺省为 6 秒
3	JX(config)#**ntp server broadcast-interval** { *interval* | **default** }	配置 ntp server 通告时间 interval：通告间隔时间，范围 3～17 秒 缺省为 6 秒
4	JX(config)#**ntp master**	指定为主时钟
5	JX(config)#**ntp stratum** *value*	配置系统时钟的层数 value：层数，范围 1～16 缺省为 16

步骤	配置	说明
6	JX(config)#**ntp unicast-peer** *peer-ipv4* { **version** *version-id* | **authentication-keyid** *key-value* | **port** *port-id* }	配置指定 ipv4 对等体 peer-ipv4：对等体 ipv4 地址 version-id：ntp 版本号 key-value：使用的认证索引 port-id：使用的 udp 端口号
7	JX(config)#**ntp unicast-server** sserver-*ipv4* { **version** *version-id* | **authentication-keyid** *key-value* | **port** *port-id* }	配置指定 ipv4 服务器 server-ipv4：服务器 ipv4 地址 version-id：ntp 版本号 key-value：使用的认证索引 port-id：使用的 udp 端口号

说明

如果设备被配置为 NTP 参考时钟源，则无法配置 NTP 服务器或 NTP 对等体；反之亦然，如果配置了 NTP 服务器或对等体，则无法将设备配置为 NTP 参考时钟源。

配置 NTP 身份验证功能

在对安全性要求较高的网络中，使用 NTP 协议时需要进行身份验证。NTP 客户端使能身份验证功能后只与通过验证的服务器进行同步，保证了网络的安全性。NTP 客户端只有使能了身份验证功能才会对服务器进行验证，若未使能身份验证功能，即使服务器携带密钥信息，客户端也不会进行验证，直接与服务器进行时间同步。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**ntp authentication { enable | disable }**	（可选）ntp 认证全局使能 enable：使能 diabale：去使能。
3	JX(config)#**ntp authentication-keyid** *key-value* **md5 key { cipher | plain }** *string*	（可选）添加 ntp 验证密钥 key-value：密钥索引值 cipher：密文 plain：明文 STRING：密钥字符串
4	JX(config)#**ntp trusted-keyid** *key-value*	（可选）指定已创建的密钥是可信的 key-value：密钥索引值

1.3.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show ntp information	显示 ntp 本地信息
2	JX#show ntp peer	显示 ntp 对端信息
3	JX#show ntp key	显示 ntp 密钥信息
4	JX#show ntp session	显示 ntp 会话信息

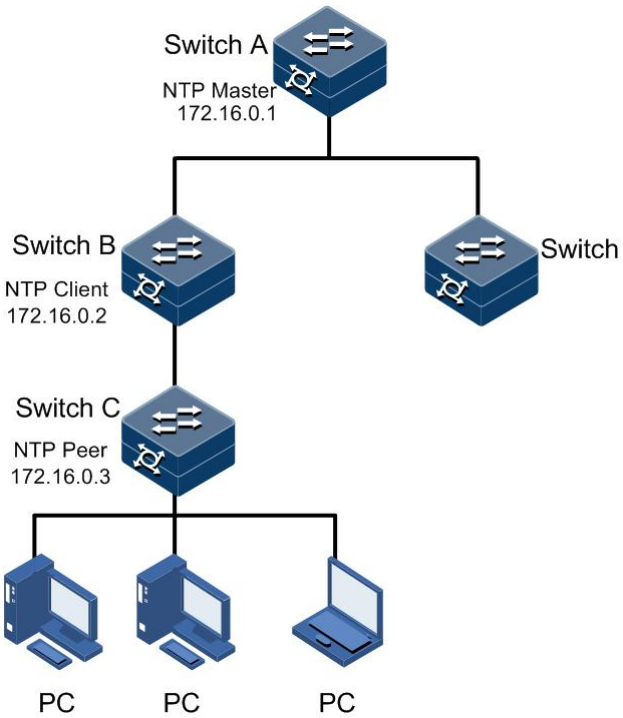
1.3.6 配置 NTP 功能示例

组网需求

某公司搭建稳定的时钟同步系统，使公司内部设备保持系统时间的一致和精准。基本规划为：

- Switch A 作为时钟同步系统的主时钟。
- Switch B 作为时钟同步系统的客户端，需设置上层的 Switch A 为 NTP 服务器。
- 设置 Switch C 为 Switch B 的 NTP 对等体，接收 Switch B 发出的下行同步数据流。

图 1-6 NTP 组网示意图



配置步骤

步骤 1 配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#ntp master
SwitchA(config-ntp)#stratum 2
```

步骤 2 配置 Switch B。

```
JX#hostname SwitchB
SwitchB#config
SwitchB(config)#ntp unicast-server 172.16.0.1
SwitchB(config)#ntp unicast-peer 172.16.0.3
SwitchB(config-ntp)#stratum 3
```

步骤 3 配置 Switch C

```
JX#hostname SwitchC
SwitchC#config
SwitchC(config)#ntp unicast-peer 172.16.0.2
SwitchC(config-ntp)#stratum 4
```

检查结果

- 查看 Switch A。

通过 **show ntp config** 查看 Switch A 配置是否正确。

```
SwitchA#show ntp config
```

- 查看 Switch B。

通过 **show ntp config** 查看 Switch B 配置是否正确。

```
SwitchB#show ntp config
```

通过 **show ntp session** 查看 Switch B 的 NTP 会话信息。

```
SwitchB#show ntp session
```

- 查看 Switch C。

通过 **show ntp config** 查看 Switch C 配置是否正确。

```
JX#show ntp config
```

通过 **show ntp session** 查看 Switch C 的 NTP 会话信息。

```
JX#show ntp session
```

1.4 PTP

1.4.1 简介

在现代通信网络中，大多数电信业务的正常运行要求全网设备之间的频率或时间差异保持在合理的误差水平内，即网络时钟同步。

网络时钟同步包括频率同步和相位同步两个概念。

频率同步（Frequency synchronization，也称为时钟同步）

频率同步，是指信号的频率保持一致，相位不一致，但是保持一定的相位差。即信号的平均速率一致，能够保持网络中的所有设备以相同的速率运行。

相位同步（Phase synchronization，也称为时间同步）

时间同步，是指信号之间的频率和相位都保持一致，即信号之间相位差恒定为零。

1588V2

IEEE1588 的全称是“网络测量和控制系统的精密时钟同步协议标准”，是通用的提升网络系统定时同步能力的规范，在起草过程中主要参考以太网来编制，使分布式通信网络能够具有严格的定时同步，并且应用于工业自动化系统。IEEE1588 主要是通过软硬件配合，记录同步时钟信息的发出时间和接收时间，并且给每一条信息加上时间标签，有了时间记录，接收方就可以计算出自己在网络中的时钟误差和延时，从而实现网络上从设备的内时钟与主控机的主时钟同步，同步建立时间可达到纳秒级的精度。与不支持 IEEE1588 的以太网延迟时间 1ms 相比，整个网络的定时同步指标有显著的改善。

最初的 IEEE1588 主要是针对局域网多播环境（如以太网）制定的标准，在电信网络的复杂环境下，IEEE1588 的应用将受到限制。因此，IEEE 从 2005 年开始制定新版本的 IEEE1588，即 IEEE1588v2。该版本最主要的是开放了 IEEE1588 的应用接口，允许其他标准组织（如 ITU-T，IETF 等）定义应用参数，即不同的 PTP 配置（profile），如 Telecom Profile。2008 年 3 月，IEEE 标准委员会通过了 IEEE1588 标准的第二版（1588v2），1588v2 协议能够提供优于 1ns 精度的时间同步，完全能够满足未来电信、工业控制、人工智能等领域内的应用。

PTP 域

应用了 PTP 协议的网络称为 PTP 域。网络中可以含有多个 PTP 域，每个 PTP 域内有且只有一个时钟源，域内的所有设备都与该时钟源保持同步。不同时钟域各有自己的同步时间，相互之间独立。

时钟节点

- 普通时钟节点（OC,Ordinary clock）

同一个 PTP 域内，只存在单个物理端口参与 PTP 时间同步的节点。设备通过该端口从上游节点同步时间，或者向下游节点发布时间。

- 边界时钟节点（BC,Boundary clock）

同一个 PTP 域内，存在两个或两个以上物理端口参与 PTP 时间同步的节点。设备通过其中一个端口从上游设备同步时间，通过其余端口向下游设备发布时间。

此外，当时钟节点作为时钟源，同时通过多个 PTP 端口向下游时钟节点发布时间，也称其为 BC。

- 透传时钟节点（TC，Transparent Clock）

TC 有多个 PTP 接口，但它只在这些接口间转发 PTP 协议报文并对其进行转发延时校正，而不会通过任何一个接口同步时间。与 BC/OC 相比，BC/OC 需要与其他时钟节点保持时间同步，而 TC 则不与其他时钟节点保持时间同步。TC 包括以下两种类型：E2ETC（End-to-End Transparent Clock，端到端透明时钟）：直接转发网络中非 P2P（Peer-to-Peer，对等）类型的 PTP 协议报文，参与计算整条链路的延时。P2PTC（Peer-to-Peer Transparent Clock，对等透明时钟）：只直接转发 Sync 报文、Follow_Up 报文和 Announce 报文，而终结其他 PTP 协议报文，参与计算整条链路上每一段链路的延时。

主从关系

PTP 域的节点设备按照一定的主从关系（Master-Slave）进行时间同步。主从关系是相对而言的，发布时间的节点设备称为主节点，同步时间的节点设备称为从节点；主节点上的时钟称为主时钟，从节点上的时钟称为从时钟；发布同步时间的端口称为主端口，接收同步时间的端口称为从端口。

一台设备可以同时从上层节点设备同步时间，然后向下层节点设备发布时间。

最优时钟

PTP 域中所有的时钟节点都按一定层次组织在一起，整个域的参考时钟就是最优时钟 GMC（Grandmaster Clock），即最高层次的时钟。通过各时钟节点间 1588v2 报文的交互，最优时钟的时间最终将被同步到整个 PTP 域中，因此最优时钟也称为该 PTP 域的时钟源。最优时钟可以通过手工配置静态指定，也可以通过最佳主时钟 BMC（Best Master Clock）算法动态选举。

时钟选源

设备支持静态选源和 BMC 选源两种方式：静态选源，通过配置选择指定时钟源为设备的主时钟源；BMC 选源，通过 BMC 算法动态选择网络中的最佳主时钟，保证设备的时钟精度。

延时机制

设备支持 E2E 延时机制和 P2P 延时机制，用于计算链路两端的时延

1.4.2 缺省配置

功能	缺省值
全局 PTP 功能	关闭
接口 PTP 功能	关闭

功能	缺省值
时钟节点类型	E2ETC
端口发包形式	组播
发送 Announce 报文的时间间隔	2s
发送 Sync 报文的时间间隔	1s

1.4.3 配置全局属性

步骤	配置	说明
1	JX(config)#**ptp start**	使能 PTP 功能
2	JX(config)#**ptp device-type** *type*	配置设备的类型

1.4.4 配置接口属性

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**ptp enable**	使能接口的 ptp
4	JX(config-ge-1/0/1)#**ptp cast-mode { multicast | unicast }**	配置接口发包模式
5	JX(config-ge-1/0/1)#**ptp delay-asymmetry** *delay*	配置接口发送报文的非对称延迟校正时间
6	JX(config-ge-1/0/1)#**ptp transport-protocol { ipv4 | ipv6 | ethernet | default }**	配置接口 PTP 的传输协议
7	JX(config-ge-1/0/1)#p**tp mac-egress dst-mac** *mac-address*	配置接口发送出的报文的封装方式为 MAC 封装
8	JX(config-ge-1/0/1)#**ptp udp-egress source-ip** *ip-address*	配置接口发送出的报文的封装方式为 UDP 封装

1.5 接口管理

1.5.1 简介

以太网接口

以太网以其高度灵活、相对简单、易于实现的特点，成为重要的局域网组网技术。以太网接口分为：以太网电接口和以太网光接口。

设备支持以太网电接口和以太网光接口。

- 自协商功能

自动协商的主要功能就是使物理链路两端的设备通过交互信息自动选择同样的工作参数。自动协商的内容主要包括双工模式、运行速率等参数。一旦协商通过，链路两端的设备就锁定在同样的双工模式和运行速率。

- 连接线缆

一般以太网标准网线分为直通线 MDI（Medium Dependent Interface）和交叉线 MDI-X（Medium Dependent Interface cross-over）两种。MDI 提供终端到网络中继设备的物理和电路连接。MDI-X 提供同种设备（终端到终端）的连接。主机和路由器的接口类型为 MDI，集线器和交换机的端口类型为 MDI-X。一般情况下，异类设备互连用直通线，同类设备互连用交叉线。自适应连接则无需考虑直通线或交叉线。

设备以太网线连接支持自适应 MDI/MDI-X。

VLAN 接口

VLAN 接口是一种逻辑接口，用于实现 VLAN 间的三层互通。每个 VLAN 对应一个 VLAN 接口，在为 VLAN 接口配置了 IP 地址后，该接口即可作为本 VLAN 内网络设备的网关，实现跨网段的报文进行基于 IP 地址的三层转发。

LoopBack 接口

LoopBack 接口是一种逻辑虚拟接口，由于该接口物理层状态和链路层协议始终处于 Up 状态，稳定性强，因此可以配置 IP 地址，并常用于动态路由协议中，作为设备的 Router ID。

NULL 接口

NULL 接口是一种逻辑虚拟接口，永远处于 Up 状态，但不能转发报文，也不能配置 IP 地址和链路层协议。NULL 接口可以对报文进行过滤，将不需要的网络流量发送到 NULL 接口，免去配置 ACL 的复杂操作。例如，在路由协议中指定到达某一网段的下一跳为 NULL 接口，则任何发送到该网段的网络数据报文都会被丢弃。

1.5.2 接口的缺省配置

设备上物理层接口的缺省配置如下。

功能	缺省值
接口的双工模式	自协商
接口的速率	自协商
接口速率统计功能状态	打开
接口的流控功能状态	禁止
接口状态	打开

1.5.3 配置接口基本属性

当互连的两个设备的接口属性，如 MTU（Maximum Transfered Unit，最大传输单元）、双工模式、速率等参数不一致时，会造成设备间无法正常通信，此时需要调整接口的属性使两端设备互相匹配。

以太网物理层分为半双工、全双工和自协商三种工作模式。

- 半双工在任意时刻只能接收或发送报文。
- 全双工在任意时刻可以同时接收和发送报文。
- 自协商是指链路两端的设备通过交互信息自动选择双工模式，一旦协商通过，两端的设备就使用同样的双工模式进行报文传输。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**description** *string*	配置接口的描述信息
4	JX(config-ge-1/0/1)#**mtu** *max-frame-length*	配置接口的最大传输单元
5	JX(config-ge-1/0/1)#**negotiation auto** { **enable** | **disable** }	配置接口自协商功能使能或关闭
6	JX(config-ge-1/0/1)#**duplex** { **full** | **half** | **default**}	配置接口的双工模式。 需要先去使能接口自协商
7	JX(config-ge-1/0/1)#**speed** { **10** | **100** | **1000** | **default**}	配置接口的速率。 对于光接口而言，接口的速率还取决于光模块的规格。
8	JX(config-ge-1/0/1)#**transceiver type** { **1000BASE-T** | **1000BASE-X** | **100GBASE-COPPER** | **100GBASE-FIBER** | **10GBASE-COPPER** | **10GBASE-FIBER** }	配置 SFP 接口连接模式。

步骤	配置	说明
9	JX(config-ge-1/0/1)#**port up-hold-time** *delay-time-value*	配置端口状态变化为 UP 时延迟处理时间
10	JX(config-ge-1/0/1)#**port down-hold-time** *delay-time-value*	配置端口状态变化为 DOWN 时延迟处理时间。

1.5.4 配置接口信息统计功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**flow-statistic interval** *time-value*	配置全局接口信息统计周期。 缺省对所有接口生效，具体接口可以配置相应命令覆盖全局
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
4	JX(config-ge-1/0/1)#**port flow-statistic interval** *time-value*	配置接口信息统计周期。 该配置覆盖全局的接口信息统计周期配置
5	JX(config-ge-1/0/1)#**reset statistics**	清除接口的统计信息。

1.5.5 配置接口流控功能

IEEE802.3x 是全双工以太网数据链路层的流量控制方法。当客户端向服务器发出请求后，自身系统或网络产生拥塞时，客户端会向服务器发出 PAUSE 帧，以延缓服务器向客户端的数据传输。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**flow-control** { **enable**| **disable** }	配置接口流控功能使能或关闭
4	JX#**show interface** *interface-type interface-number*	查询接口详细信息，查看流控功能使能状态。

1.5.6 配置接口打开或关闭

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式/VLAN 接口配置模式/链路聚合接口配置模式。
3	JX(config-ge-1/0/1)#**shutdown**	关闭当前接口。 可以使用 **no shutdown** 命令再次打开接口。

1.5.7 配置接口允许通过的 tagged 报文类型

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式/链路聚合接口配置模式。
3	JX(config-ge-1/0/1)#**accept-frame-type** { **all** | **only-tagged** }	all：配置接口 tagged 和 untagged 报文通过。 only-tagged:配置接口只允许 tagged 报文通过。 缺省是 all。

1.5.8 配置管理报文优先级

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式
3	JX(config-vlanif-*)#**packet-priority 8021p** *value*	配置报文优先级。
4	JX(config-vlanif-*)#**no packet-priority 8021p**	恢复报文缺省优先级

1.5.9 查看接口统计

请在设备上进行以下配置。

步骤	配置	说明
1	JX#show **interface** *interface-type interface-number*	查看以太网接口详细信息，包括统计信息
2	JX#show **interface ethernet** [**statistics**]	查看所有以太网接口统计信息
3	JX#show **interface vlan** [statistics]	查看所有 VLAN 接口的统计信息

1.5.10 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show interface**	查看接口列表概要信息。
2	JX#**show interface verbose**	查看接口列表详细信息。
3	JX#**show interface** *interface-type interface-number*	查看具体接口的详细信息
4	JX#**show interface** *interface-type interface-number* **config**	查看接口配置信息。

2 以太网

本章介绍以太网特性的原理和配置过程，并提供相关的配置案例。

- MAC 地址转发表
- VLAN
- Voice VLAN
- QinQ
- VLAN 转换
- MRP/MVRP

2.1 MAC 地址转发表

2.1.1 简介

以太网设备转发以太网报文是通过 MAC 地址转发规则实现的快速转发，每台设备都有一个 MAC 地址与每个接口的转发对应表，这就是 MAC 地址转发表。所有入接口报文都会依据 MAC 地址转发表进行转发，是以太网设备实现二层报文快速转发的基础。MAC 地址转发表存储在设备的缓存中，缓存容量决定设备能存储多少 MAC 地址。

MAC 地址转发表的表项中包含如下信息：

- 目的 MAC 地址
- 目的 MAC 地址所对应的接口号
- 接口所属的 VLAN ID
- 标志位 Flag

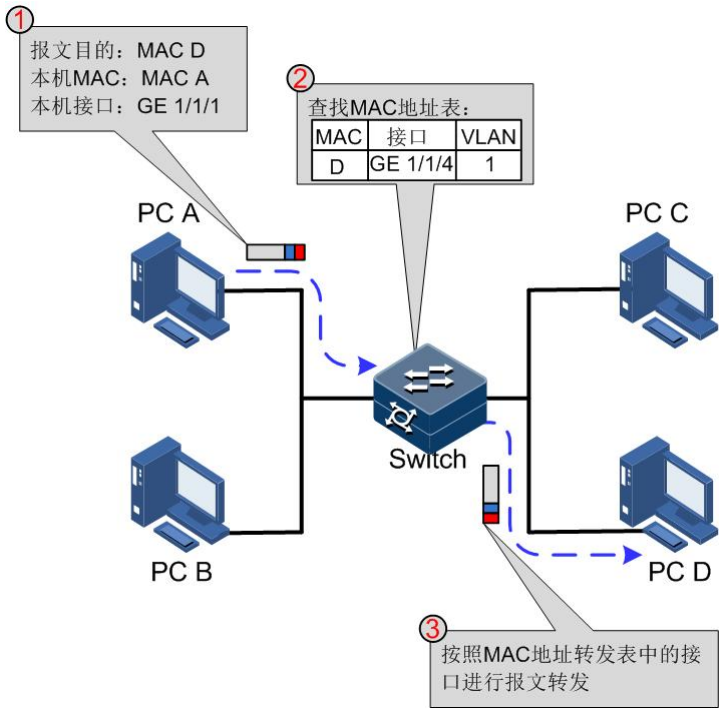
设备可基于设备、接口和 VLAN 来查看 MAC 地址表信息。

MAC 地址转发方式

以太网设备在转发报文时，根据 MAC 地址表项信息，会采取以下转发方式：

- 单播方式：当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，设备直接将报文从该表项中的转发接口发送；如不包含对应表项，则以广播方式向除接收接口外的所有接口转发。如下图所示。

图 2-1 MAC 地址表转发示意图



- 组播方式：当设备收到目的地址为组播 MAC 地址的报文时，组播以广播形式发送，如果开启了组播功能并设置了未知组播过滤，则发送到指定 Report 接口。如无指定 Report 接口，则报文丢弃不转发。
- 广播方式：当设备收到目的地址为全 F 的报文，或 MAC 地址转发表中没有包含对应报文目的 MAC 地址的表项时，设备将采取广播方式将报文向除接收接口外的所有接口转发。

MAC 地址表项的分类

MAC 地址转发表分为静态地址表和动态地址表两项。

- 静态 MAC 地址表项：也称为“永久地址”，由用户手工添加和删除，不会随着时间老化。对于一个设备变动较小的网络，手工添加静态地址表项可以减少网络中的广播流量，能够提高接口的安全性，且系统复位后，表项不丢失。
- 动态 MAC 地址表项：交换机可以通过 MAC 地址学习机制学习动态 MAC 地址表项，该表项会按照用户配置的老化时间而老化掉。系统复位后，表项会清空。

MAC 地址老化时间

以太网交换机的 MAC 地址转发表是有容量限制的。为了最大限度利用地址转发表资源，以太网交换机利用老化机制更新 MAC 地址转发表，即：系统在动态创建某条表

项的同时，开启老化定时器，如果在老化时间内没有再次收到来自该表项中的 MAC 地址的报文，交换机就会把该 MAC 地址表项删除。

设备支持 MAC 地址自动老化，老化时间设置范围为 0 或 60s～1000000s，其中 0 表示永不老化。

说明

MAC 地址的老化机制只对动态 MAC 地址表项生效。

MAC 地址转发策略

MAC 地址转发表有 2 种转发策略：

- 当报文进入设备接口时，会在 MAC 地址表查找报文中的目的 MAC 地址所关联的接口，如果在 MAC 地址表中有目的 MAC，并且目的 MAC 对应的接口与报文进入设备的接口不同，则从目的 MAC 对应的接口转发报文，并会将报文中的源 MAC 地址记录下来，与入报文的接口号、VLAN ID 相关联记录到 MAC 地址表中。当其它接口有去往该 MAC 地址时，可以通过 MAC 对应表将报文直接转发到对应的接口。
- 如果在 MAC 地址表中没有这个报文的目的 MAC，就会向除源接口外所有相同广播域的接口转发数据包，并记录该数据包中的源 MAC 地址到设备 MAC 地址表中。

MAC 地址学习数目限制

MAC 地址学习数目限制功能主要是为了限制 MAC 地址条目数，避免了因 MAC 地址表过于庞大，可能延长查找转发表项的时间，导致以太网交换机的转发性能下降的情况，是一种管理 MAC 地址表的有效方法。

MAC 地址学习数目限制主要用于限制 MAC 地址转发表的大小，提高交换机芯片的转发速度。

2.1.2 配置准备

场景

在以下情况，需要配置静态 MAC 地址转发表：

- 在公司内固定服务器、以及特定人员（经理、财务等）位置相对固定且较重要的主机上配置固定的静态 MAC 地址。以保证所有去往该 MAC 地址的数据流优先从静态 MAC 地址对应的接口进行转发。
- 对于固定静态 MAC 地址的接口，可以设置禁止 MAC 地址学习，防止其他主机通过该接口访问局域网数据。

同时，为避免 MAC 地址转发表中保存过多的 MAC 地址表项，而耗尽 MAC 地址表资源，需要配置 MAC 地址转发表的老化时间，以实现动态 MAC 地址的老化功能。

前提

无

2.1.3 MAC 地址转发表的缺省配置

设备上 MAC 地址转发表的缺省配置如下。

功能	缺省值
MAC 地址学习功能状态	使能
MAC 地址老化时间	300s
MAC 地址学习数目限制	无限制
MAC 地址漂移检测	使能
MAC 地址漂移保护	关闭

2.1.4 配置静态 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**mac-address static vlan** *vlan-id* **mac** *mac-address interface-type interface-number*	配置静态单播 MAC 地址

说明

设备的 MAC 地址、组播地址、FFFF.FFFF.FFFF 及 0000.0000.0000 不能被配置为静态单播 MAC 地址。

2.1.5 配置黑洞 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**mac-address blackhole vlan** *vlan-id* **mac** *mac-address*	配置黑洞 MAC 地址。

2.1.6 配置 MAC 地址学习

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**mac-address learning** { **disable** | **enable** }	使能或禁止 MAC 地址学习功能

2.1.7 配置基于 VLAN 的 MAC 地址学习

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置模式。
3	JX(config-vlan-10)#**mac learning** { **disable** | **enable** }	使能或禁止 MAC 地址学习功能

2.1.8 配置 MAC 地址学习数目限制

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**mac-limit** *limit-value*	配置接口下 MAC 地址学习数目限制阈值。

2.1.9 配置 MAC 老化时间

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**mac-address aging-time** { **0** | **default** | *period* }	配置 MAC 地址老化时间。

2.1.10 配置 MAC 地址漂移检测与保护

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**mac-address flapping detection** { **enable** | **disable** }	使能或关闭 MAC 地址漂移检测功能
3	JX(config)#**mac-address flapping detection exclude-vlan** *vlan-list*	配置不检测 MAC 地址漂移的 VLAN
4	JX(config)#**mac-address flapping detection vlan** *vlan-list* **security-level** { **high** | **middle** | **low** }	配置检测 MAC 地址漂移的 VLAN 并配置触发 MAC 地址漂移保护的安全等级 安全等级越高，触发漂移保护需要的 MAC 地址漂移次数越少
5	JX(config)#**mac-address flapping error-down recovery-interval** *period*	配置 MAC 地址漂移触发接口 error-down 的自动恢复的时间
6	JX(config)#**mac-address flapping quit-vlan recover-time** *period*	配置 MAC 地址漂移触发接口 quit-vlan 的自动恢复的时间
7	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
8	JX(config-ge-1/0/1)#**mac-address flapping action** { **error-down** | **quit-vlan** }	配置接口下 MAC 地址漂移保护动作
9	JX(config-ge-1/0/1)#**mac-address flapping action priority** *priority*	配置接口下 MAC 地址漂移保护动作的端口优先级 优先级数值越高，优先触发保护动作

2.1.11 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show mac-address**	查看 MAC 地址表项信息。
2	JX#**show mac-address vlan** *vlan-id*	查看指定 VLAN 的 MAC 地址表项信息。
3	JX#**show mac-address interface** *interface-type interface-number*	查看指定接口的 MAC 地址表项信息。

序号	检查项	说明
3	JX#**show mac-address { static | dynamic | blackhole }** [**vlan** *vlan-id*]	查看静态/动态/黑洞 MAC 地址表项信息。
4	JX#**show mac-address aging-time**	查看 MAC 地址老化时间。
5	JX#**show mac-address flapping record**	查看 MAC 地址漂移检测记录。
6	JX#**show mac-limit** [**interface** *interface-type interface-number*]	查看 MAC 地址学习数目限制的配置信息。

2.1.12 维护

用户可以通过以下命令维护 MAC 地址转发表特性。

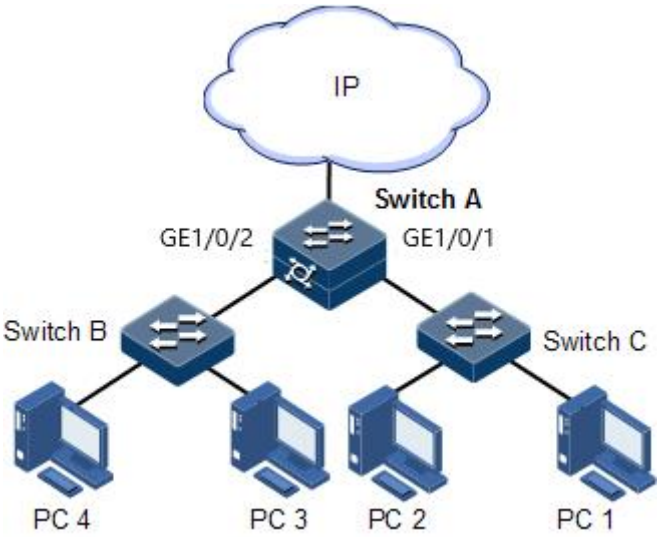
命令	描述
JX(config)#**no mac-address** [**vlan** *vlan-id*] [**mac** *mac-address*]	清除指定参数的 MAC 地址。
JX(config)#**no mac-address** *interface-type interface-number*	清除指定接口的 MAC 地址。
JX(config)#**no mac-address { static | dynamic | blackhole }** [**vlan** *vlan-id*] [**mac** *mac-address*]	清除指定参数的静态/动态/黑洞 MAC 地址
JX(config)#**no mac-address { static | dynamic }** [*interface-type interface-number*]	清除指定接口的静态/动态 MAC 地址
JX(config)#**reset mac-address flapping record**	清除 MAC 地址漂移记录

2.1.13 配置 MAC 地址转发表示例

组网需求

如下图所示，在 Switch A 上进行操作，在 GE 1/0/2 配置一条静态单播 MAC 地址 0001.0203.0405，所属 VLAN 为 VLAN 10；配置 MAC 地址老化时间为 500s。

图 2-2 MAC 应用组网示意图



配置步骤

步骤 1 创建 VLAN 10 并激活，将 GE 1/0/2 加入 VLAN 10。

```
JX#config
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
```

步骤 2 在 GE 1/0/2 配置一条静态单播 MAC 地址 0001.0203.0405，所属 VLAN 10。

```
JX(config)#mac-address static vlan 10 mac 00:01:02:03:04:05 ge 1/0/2
```

步骤 3 配置 MAC 地址老化时间为 500s。

```
JX(config)#mac-address aging-time 500
```

检查结果

通过 **show mac-address** 命令查看 MAC 地址配置。

```
JX#show mac-address
  MacAddress        VLAN/VSI/BD Learned-From    Type       Valid
------------------------------------------------------------------------------
  0001:0203:0405     10/--/--    ge-1/0/2       static     yes
------------------------------------------------------------------------------
  Total:1      Static:1       Dynamic:0      Blackhole:0
  Sticky:0     Security:0     Snooping:0
```

2.2 VLAN

2.2.1 简介

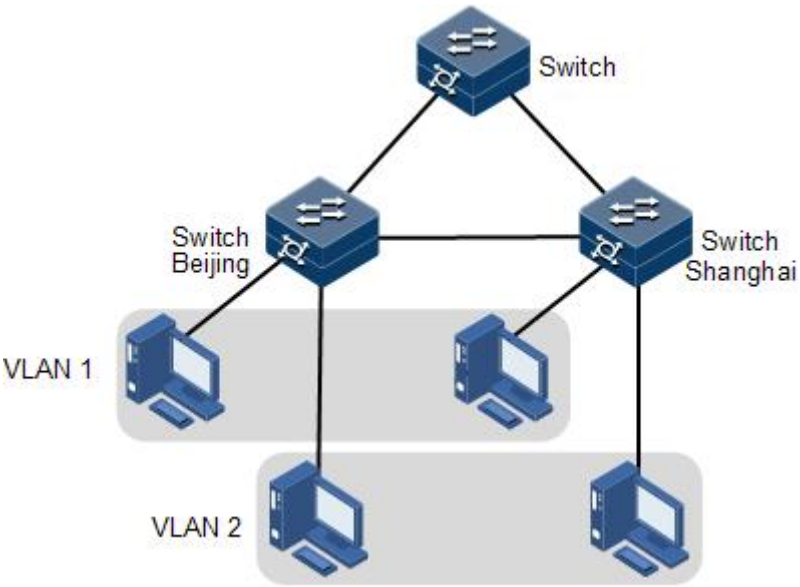
VLAN 概述

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议。它是一种通过将局域网内的设备逻辑地而不是物理地划分成不同的广播域，从而实现多个互不影响的虚拟工作组的二层隔离技术。从功能上看，VLAN 和 LAN 有着相同的特性，但两者的主要区别在于同一 VLAN 内的成员可以不受物理位置的限制进行相互访问。

VLAN 划分

VLAN 划分有多种方式，例如基于接口、基于 MAC 地址、基于 IP 子网、基于协议划分等，如下图所示。

图 2-3 VLAN 划分示意图



VLAN 技术允许将一个物理的 LAN 逻辑地划分成不同的广播域。通过划分 VLAN，将没有互通需求的主机进行隔离，在增强网络安全性、减少广播流量的同时也减少了广播风暴的发生。

设备符合 IEEE 802.1Q 标准的 VLAN，支持 4094 个并发 VLAN。

- 基于接口划分 VLAN

设备支持基于接口划分 VLAN。交换机设备的接口模式分为 Access 和 Trunk 两种，接口模式与报文转发处理方式比较请参考下表。

表 2-1 接口模式与报文转发

接口类型	入报文处理		出报文处理
	Untag 报文	带 Tag 报文	
Access	为报文打上 Access VLAN 的 Tag	• 报文 VLAN ID＝Access VLAN ID，接收该报文 • 报文 VLAN ID≠Access VLAN ID，丢弃该报文	• 报文 VLAN ID＝Access VLAN ID，去掉 Tag 发送该报文 • 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文
Trunk	为报文打上 Native VLAN 的 Tag	• 接口允许通过的 VLAN ID 列表中包含报文 VLAN ID，接收该报文 • 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文	• 报文 VLAN ID＝Native VLAN ID，去掉 Tag 发送该报文 • 报文 VLAN ID≠Native VLAN ID，且接口允许通过时，保持原有 Tag 发送该报文
Hyjbrid	为报文打上缺省 VLAN 的 Tag	• 接口允许通过的 VLAN ID 列表中包含报文 VLAN ID，接收该报文 • 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文	• 接口允许通过的 VLAN ID 列表中包含报文 VLAN ID，发送该报文，可以通过命令设置发送时是否携带 Tag • 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文

- 基于 MAC 地址划分 VLAN

基于 MAC 地址划分 VLAN 是指根据报文源 MAC 地址对 VLAN 进行划分。

  - 当接口收到的报文为 Untag 报文时，根据报文的源 MAC 地址匹配 MAC VLAN 表项。如果报文中的源 MAC 地址与 MAC VLAN 表项中的 MAC 地址完全相同，则匹配成功，给报文添加表项中指定的 VLAN ID 并转发该报文。如果没有找到匹配 MAC VLAN 表项，则继续匹配基于 IP 子网 VLAN、基于接口 VLAN。
  - 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。

- 基于 IP 子网划分 VLAN

基于 IP 子网划分 VLAN 是指根据报文源 IP 地址及子网掩码对 VLAN 进行划分。

  - 设备从接口接收到 Untag 报文后，会根据报文的源 IP 地址及子网掩码确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。
  - 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。

- 基于协议划分 VLAN

基于协议划分 VLAN 是指根据数据帧所属的协议类型及封装格式对 VLAN 进行划分。

- 设备从接口接收到 Untag 报文后，会根据报文的协议域确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。
- 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。

2.2.2 配置准备

场景

VLAN 最主要功能是划分逻辑网段，通常有 2 种典型应用模式。

- 一种是在小型局域网中，一台设备下划分多个 VLAN，用 VLAN 将所有连接到设备的主机逻辑的划分开，同一个 VLAN 内的主机之间可以相互通信，不同 VLAN 间的主机之间无法通信。例如财务部门与其他部门需要划分开，互相不能访问，通常连接主机的接口设置为 Access 模式。
- 另一种是在稍大型局域网或企业网中，有多台设备连接较多的主机，并且设备之间级联，转发数据报文时都携带 VLAN Tag，多台设备的相同 VLAN 的接口可以相互通信，不同 VLAN 的主机之间无法通信。主要用在公司人员及主机数量较多，并且同一个部门所在位置不同，但是要求部门内的主机可以互相访问，需要在多台设备上划分 VLAN。如果不同 VLAN 之间需要通信，则要通过路由器等 3 层设备。设备之间级联的接口设置为 Trunk 模式。

当需要为 VLAN 配置 IP 地址时，可以为其关联一个三层接口，每一个三层接口将对应一个 IP 地址并关联一个 VLAN。

前提

无

2.2.3 VLAN 的缺省配置

设备上 VLAN 的缺省配置如下。

功能	缺省值
创建 VLAN	存在 VLAN 1
接口模式	Hybrid
PVID	1
Trunk 接口的 VLAN	VLAN 1
Access 接口的 VLAN	VLAN 1

2.2.4 配置 VLAN 属性

请在需要配置 VLAN 属性信息的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-list*	创建 VLAN。 该命令也可用于批量创建 VLAN。
3	JX(config)#**vlan** v*lan-id*	进入 VLAN 配置模式。

说明

- 用 **vlan** *vlan-id* 命令新创建的 VLAN 为活动状态。
- VLAN 的所有配置仅在该 VLAN 被激活后才会在系统中生效。

2.2.5 配置接口模式

请在需要配置接口模式的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**port link-type** { **access** | **default** | **dot1q-tunnel** | **hybrid** | **trunk** }	配置接口模式为 Access 或 Trunk 或 hybrid 或 dotq-tunnel。

2.2.6 配置基于 Access 接口的 VLAN

请在需要配置基于 Access 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以二层物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**port link-type accsess** JX(config-ge-1/0/*)#**port default vlan** *vlan-id*	配置接口模式为 Access，并将 Access 接口加入 VLAN。

说明

- 无论 Access 接口允许通过的 VLAN 列表如何配置，该接口都允许 Access VLAN 的数据包通过，且转发出去的数据包不携带相应 VLAN TAG 标记。
- 设置 Access VLAN 时，如果该 VLAN 没有创建并激活，将无法配置成功。
- 如果 Access VLAN 被用户手动删除或挂起，系统不会自动设置该接口 Access VLAN 为缺省 VLAN。
- 当配置接口 Access VLAN 为非缺省的 Access VLAN 时，缺省 Access VLAN 1 为 Access 出接口允许通过的 VLAN，通过配置删除 Access 出接口允许通过的 VLAN，可以将缺省 Access VLAN 1 从 Access 出接口允许通过 VLAN 列表中删除。
- 如果配置 Access VLAN 不是缺省 VLAN，且 Access 接口允许通过的 VLAN 列表中没有缺省 VLAN，该接口将不允许缺省 VLAN 的数据包通过。

2.2.7 配置基于 Trunk 接口的 VLAN

请在需要配置基于 Trunk 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**port link-type trunk**	配置接口模式为 Trunk。
4	JX(config-ge-1/0/*)#**port trunk pvid** *vlan-id*	配置接口 PVID。
5	JX(config-ge-1/0/*)#**port trunk allowed-pass vlan** { **all** | *vlan-list* }	配置 Trunk 接口允许通过的 VLAN。

- 无论 Trunk 接口允许通过的 VLAN 列表列表如何配置，该接口都允许 VLAN 的数据包通过，且转发出去的数据包不携带相应 PVID 标记。
- 设置 Native VLAN 时，如果该 VLAN 没有创建并激活，系统不会自动创建并激活该 VLAN。
- 如果 Native VLAN 被用户手动删除或阻塞，系统不会自动设置该接口 Trunk Native VLAN 为缺省 VLAN。
- 接口允许 Trunk Allowed VLAN 报文出入。
- 如果配置 Native VLAN 不是缺省 VLAN，且 Trunk 接口允许通过的 VLAN 列表中没有缺省 VLAN，该接口将不允许缺省 VLAN 的数据包通过。
- Trunk 允许 VLAN 列表都只对静态 VLAN 生效，对集群 VLAN、GVRP 动态 VLAN 等不生效。

2.2.8 配置基于 Hybrid 接口的 VLAN

请在需要配置基于 Hybrid 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**port link-type hybrid**	配置接口模式为 hybrid。
4	JX(config-ge-1/0/*)#**port hybrid pvid** *vlan-id*	配置接口 PVID。
5	JX(config-ge-1/0/*)#**port hybrid vlan** { **all** | *vlan-list* } { **tagged** | **untagged** }	配置 hybrid 接口以{tagged|untagged}方式允许通过的 VLAN。

- Hybrid 端口根据配置的不同将有不同的工作方式，untagged 方式接口工作模式与 Access 模式端口相同，但可配置多个可通过 VLAN，tagged 方式接口工作模式与 trunk 模式端口相同。

2.2.9 配置基于 MAC 地址的 VLAN

请在需要配置基于 MAC 地址的 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**mac-vlan** *mac-address vlan-id*	配置 MAC 地址与 VLAN 的关联
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	JX(config-ge-1/0/*)#**mac-vlan enable**	使能 MAC-VLAN 功能。

注意

- MAC 地址为组播 MAC 地址、全 0 或全 F 时，配置失败。
- 创建的 MAC 地址与 VLAN 关联与已经存在的关联冲突（例如同一 MAC 地址关联到不同的 VLAN），则配置失败。

2.2.10 配置基于 IP 子网的 VLAN

请在需要配置基于 IP 子网的 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**ip-subnet-vlan** *ip-address* [*ip-mask*] **vlan** *vlan-id*	配置 VLAN 与 IP 子网地址的关联。
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	JX(config-ge-1/0/*)#**ip-subnet-vlan enable**	使能基于 IP 子网划分 VLAN 功能。

注意

- IP 地址或掩码无效时，配置失败。
- 创建的 IP 子网与 VLAN 关联与已经存在的关联冲突（例如同一子网关联到不同的 VLAN 时），配置失败。

2.2.11 配置基于协议的 VLAN

请在需要配置基于协议划分 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**protocol-vlan** *protocol-index* { **ethernet2** | **llc** | **snap** *protocol-id* }	配置协议 VLAN 与以太报文关联规则
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	JX(config-ge-1/0/*)#**protocol-vlan** *protocol-index* **vid** *vlan-id*	配置接口和协议 VLAN 的关联规则

2.2.12 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show vlan** [*vlan-list* | *vlan-id*]	查看 VLAN 配置。
2	JX#**show port vlan**	查看接口 VLAN 配置信息。
3	JX#**show mac-vlan** [*vlan-id*]	查看 MAC VLAN 配置信息
4	JX#**show ip-subnet-vlan** [*vlan-id*]	查看 IP 子网 VLAN 的配置信息。
5	JX#**show protocol-vlan all**	查看全部协议 VLAN 配置信息。
6	JX#**show protocol-vlan interface**	查看接口的协议 VLAN 配置信息。

2.2.13 查询 VLAN 统计信息

查询 VLAN 统计，请在设备上执行以下命令获取统计结果。

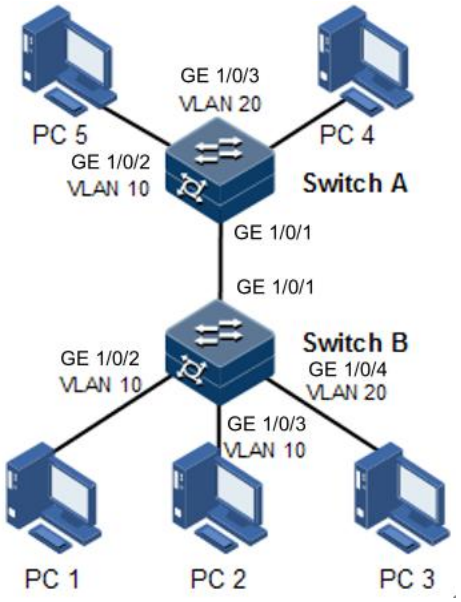
序号	检查项	说明
1	JX(config-vlan-*)#**statistics { enable | disable }**	使能 VLAN 统计功能。
2	JX#**show vlan** [*vlan-id*] **statistics**	查看 VLAN 统计信息。
3	JX(config)#**reset vlan** [*vlan-id*] **statistics**	清除 VLAN 统计信息。

2.2.14 配置 VLAN 示例

组网需求

如图 2-4 所示，PC 1、PC 2、PC 5 属于 VLAN 10，PC3、PC4 属于 VLAN 20；两台设备相连的接口为 Trunk 模式，但不允许 VLAN 20 的报文通过，使 PC 3 和 PC 4 无法通信；在同一 Switch B 设备下的 PC 1 和 PC 2 的接口开启接口保护功能，使 PC 1 和 PC 2 无法通信，但 PC 1 和 PC 2 分别可以和 PC 5 通信。

图 2-4 VLAN 和接口保护组网示意图



配置步骤

步骤 1 在两台设备上分别创建 VLAN 10 和 VLAN 20 并激活。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 10,20
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#configure
SwitchB(config)#vlan 10,20
```

步骤 2 将 Switch B 的接口 GE 1/0/2 和 GE 1/0/3 以 Access 模式加入 VLAN 10，接口 GE 1/0/4 以 Access 模式加入 VLAN 20，接口 GE 1/0/1 为 Trunk 模式允许 VLAN 10 通过。

```
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#port link-type access
SwitchB(config-ge-1/0/2)#port default vlan 10
```

```
SwitchB(config-ge-1/0/2)#exit
SwitchB(config)#interface ge 1/0/3
SwitchB(config-ge-1/0/3)#port link-type access
SwitchB(config-ge-1/0/3)#port default vlan 10
SwitchB(config-ge-1/0/3)#exit
SwitchB(config)#interface ge 1/0/4
SwitchB(config-ge-1/0/4)#port link-type access
SwitchB(config-ge-1/0/4)#port default vlan 20
SwitchB(config-ge-1/0/4)#exit
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#port trunk allow-pass vlan 10
SwitchB(config-ge-1/0/1)#exit
```

步骤 3 将 Switch A 的接口 GE 1/0/2 以 Access 模式加入 VLAN 10，接口 GE 1/0/3 以 Trunk 模式加入 VLAN 20，接口 GE 1/0/1 为 Trunk 模式允许 VLAN 10 通过。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type access
SwitchA(config-ge-1/0/2)#port access vlan 10
SwitchA(config-ge-1/0/2)#exit
SwitchA(config)#interface ge 1/0/3
SwitchA(config-ge-1/0/3)#port mode trunk
SwitchA(config-ge-1/0/3)#port trunk pvid 20
SwitchA(config-ge-1/0/3)#port trunk allow-pass 20
SwitchA(config-ge-1/0/3)#exit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allowed-pass vlan 10
```

检查结果

通过 **show vlan** 命令查看 VLAN 的配置信息是否正确。

以 Switch B 为例。

```
SwitchB#show vlan

    S: supervlan       P: pvlan        N: normal


 Vlan  Type       Ports('M': member , '-': not member)
--------------------------------------------------------------------------------
 1    N/static    untagged: ge-1/0/1<->ge-1/0/16      M---MMMM MMMMMMMM
                          ge-1/0/17<->ge-1/0/24       MMMMMMMM
                          10ge-1/0/25<->10ge-1/0/30   MMMMMM
 10   N/static    tagged:   ge-1/0/1<->ge-1/0/16      M------- --------
                  untagged: ge-1/0/1<->ge-1/0/16      -MM----- --------
 20   N/static    untagged: ge-1/0/1<->ge-1/0/16      ---M---- --------
--------------------------------------------------------------------------------
```

```
  Total: 3    Static: 3    Dynamic: 0
```

通过 **show interface** *interface-type interface-number* 查看接口 VLAN 配置是否正确。

以 Switch B 为例。

```
SwitchB#show interface ge 1/0/2 config
!
interface ge 1/0/2
 port link-type access
 port default vlan 10
```

通过 PC 1 ping PC 5、PC 2 ping PC 5、PC 3 ping PC 4 是否能够 ping 通，查看 Trunk 接口允许通过 VLAN 是否正确。

- PC 1 ping PC 5，可以 ping 通，VLAN 10 通信正常
- PC 2 ping PC 5，可以 ping 通，VLAN 10 通信正常
- PC 3 ping PC 4，不能 ping 通，VLAN 20 无法通信

2.3 Voice VLAN

2.3.1 简介

随着语音技术的日益发展，语音设备应用越来越广泛，尤其在宽带小区，网络中经常同时存在语音、数据和业务数据两种流量。语音数据在传输时需要具有比业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。

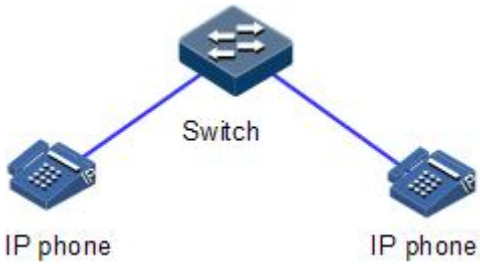
Voice VLAN 指为用户的语音数据流而专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以为语音数据配置 QoS（Quality of Service，服务质量），提高语音流量的传输优先级，保证通话质量。

相对于使用其他语音流的方法，Voice VLAN 对语音流的管理具有以下一些优势：

- 配置简单：用户只需要在全局和端口下进行简单的配置，开启 Voice VLAN 功能，即可对语音数据进行分类处理。
- 便于维护：用户可以在全局配置对语音数据的匹配规则（Voice VLAN OUI 地址）进行修改，在新增 IP 语音设备的情况下，各端口能够迅速根据更新的匹配规则识别语音流。
- 实现灵活： Voice VLAN 功能在全局提供了安全/普通两种模式，端口上又可以分为自动/手动模式，实现更为灵活，用户可以根据自己需要进行组合，最大限度满足用户的需求。

适用于 IP 电话单独接入交换机（端口仅传输语音报文）的组网方式（如图 2 所示），这种静态加入的方式可以使该端口专用于传输语音数据，最大限度避免业务数据对语音数据传输的影响。

图 2-5 IP 电话单独接入交换机组网示意图



2.3.2 配置准备

场景

语音流量可通过专属 VLAN（Voice VLAN）传输，在一段时间内，如果语音设备发生故障或语音设备退出网络，连接语音设备的端口会自动从 Voice VLAN 中退出。

前提

已经创建 VLAN，并且正确设备 VLAN 属性。

2.3.3 Voice VLAN 的缺省配置

设备上 Voice VLAN 的 OUI（Organizationally Unique Identifier，全球统一标识符地址）缺省配置如下。

OUI-Address	Mask address	Description
0001.E300.0000	FFFF.FF00.0000	Siemens-phone
0003.6B00.0000	FFFF.FF00.0000	Cisco-phone
0004.0D00.0000	FFFF.FF00.0000	Avaya-phone
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone
00E0.7500.0000	FFFF.FF00.0000	Verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone

设备上 Voice VLAN 的其他缺省配置如下。

功能	缺省值
Voice VLAN 功能	禁止
Voice Vlan 工作模式为安全模式	禁止
Voice Vlan 工作模式为普通模式	使能

功能	缺省值
端口加入 Voice Vlan 的工作模式为自动模式	禁止
端口加入 Voice Vlan 的工作模式为手工模式	禁止
Voice Vlan 报文的 Cos 和 DSCP 值	Voice VLAN 报文 COS 为 6，DSCP 为 46
Voice Vlan QoS 优先级信任	无
Voice Vlan 老化时间	5min

2.3.4 配置 OUI 地址

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**voice-vlan oui** *mac-address* [*mask-address*] [*description word*]	配置 Voice VLAN 的 OUI。

2.3.5 使能 Voice VLAN 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	JX(config-ge-1/0/*)#**voice-vlan** *vlan-id* **enable**	配置 Voice VLAN 功能使能。
4	JX(config-ge-1/0/*)#**voice-vlan mode** { **auto** | **manual** }	配置端口加入 Voice VLAN 的工作模式。
5	JX(config)#**voice-vlan aging-time** *time*	配置端口在自动模式下离开 Voice VLAN 的老化时间。
6	JX(config)#**interface** *interface-type interface-number* JX(config-ge-1/0/*)#**voice-vlan security** { **enable** | **disable** }	配置 Voice Vlan 工作模式为安全模式。

2.3.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show voice-vlan oui	查看当前设备上的 OUI 地址、OUI 地址掩码和描述信息。
2	JX#show voice-vlan interface	查看当前设备上 Voice VLAN 的接口状态。

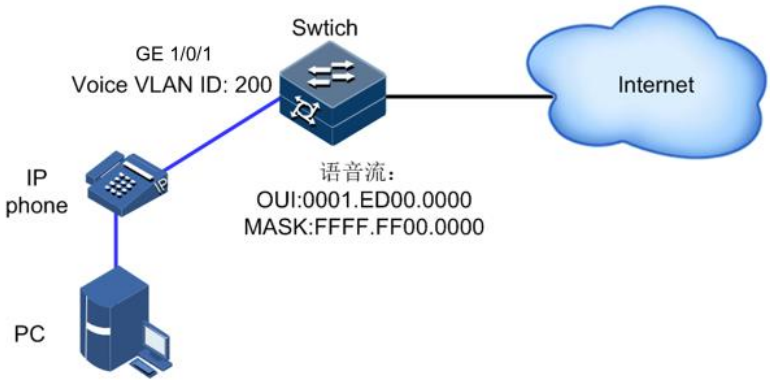
2.3.7 配置端口加入 Voice VLAN 示例

配置端口加入 Voice VLAN，工作于手动模式

组网需求

Switch 的 GE 1/0/1 接口接入 IP 电话和 PC，要求 GE 1/0/1 端口同时转发并且隔离语音流和数据流。

可将端口配置为 Trunk 口，Native Vlan 转发数据流，Voice Vlan 转发语音流。PC 发出的是 Untagged 的报文，因此会在端口的 Native VLAN 内传输，将 Native Vlan 设置为 100，用来传输 PC 发出的数据流；IP 电话发出的也是 Untagged 报文，源 mac 配置为 Voice Vlan 的 OUI 地址，则报文通过 Voice Vlan 端口时会添加 Voice Vlan Tag，Voice Vlan 设置为 200，用来传输 IP 电话语音流。



配置步骤

步骤 1 在交换机上设置 IP Phone 的 MAC 地址（支持掩码）为 Voice Vlan OUI 地址，地址为 0001.ED00.0000，掩码是 FFFF.FF00.0000。设备默认支持的 OUI 参见 VoiceVLAN 缺省配置章节。

```
JX(config)#voice-vlan oui 00:01:ED:00:00:00/24
```

步骤 2 创建 VLAN100，VLAN200 并激活，设置 VLAN 200 为 Voice VLAN。

```
JX(config)#vlan 100,200
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
```

```
JX(config-ge-1/0/1)#port trunk allow-pass vlan 100
JX(config-ge-1/0/1)#voice-vlan 200 enable
```

检查配置

使用命令 **show voice-vlan interface** 查看设备当前的 Voice VLAN 接口状态

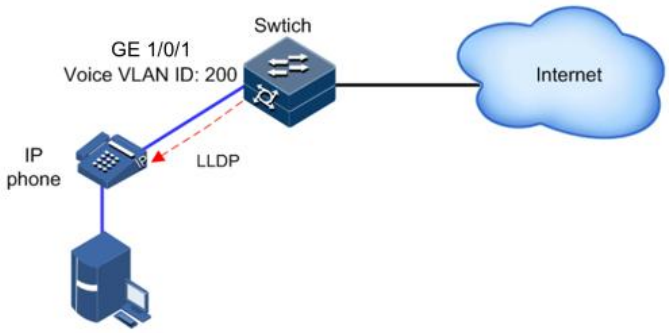
```
JX(config)#show voice-vlan interface
  Support max interface      :64
  Current enable interface   :1
  Interface        VID    Mode    Security  RemainTime(s)
------------------------------------------------------------
  ge-1/0/1         200      auto   enable    N/A
------------------------------------------------------------
```

2.3.8 配置 LLDP 实现 IP 话机接入 Voice VLAN 示例

组网需求

当语音设备支持 LLDP 协议，如图所示，支持通过 LLDP 协议获取语音 VLAN。因此可通过在交换机上配置 LLDP 和 Voice VLAN 功能，实现 IP 话机接入。在交换机上通过配置 LLDP 协议向语音设备发布端口的 Voice VLAN；为保证通话质量，配置 Voice VLAN 功能提升语音报文的优先级。

Switch 的 GE 1/0/1 接口接入 IP 电话和 PC，要求 GE 1/0/1 端口同时转发并且隔离语音流和数据流。可将端口可配置为 Trunk 口，Native Vlan 转发数据流，Voice Vlan 转发语音流。PC 发出的是 Untagged 的报文，因此会在端口的 Native VLAN 内传输，将 Native Vlan 设置为 100，用来传输 PC 发出的数据流；Voice Vlan 设置为 200，用来传输 IP 电话语音流，IP 电话通过 LLDP 协议获取到 Voice VLAN，发出的是带 Voice VLAN Tag 的报文。



配置步骤

步骤 1 在交换机上设置 IP Phone 的 MAC 地址（支持掩码）为 Voice Vlan OUI 地址，地址为 0001.ED00.0000，掩码是 FFFF.FF00.0000。设备默认支持的 OUI 参见 VoiceVLAN 缺省配置章节。

```
JX(config)#voice-vlan oui 0001.ED00.0000/24
```

步骤 2 创建 VLAN100，VLAN200 并激活，设置 VLAN 200 为 Voice VLAN。

```
JX(config)#vlan 100,200
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 100
JX(config-ge-1/0/1)#voice-vlan 200 enable
JX(config-ge-1/0/1)#exit
```

步骤 3 全局和接口使能 LLDP 功能，向 IP 话机发布端口的 Voice VLAN。

```
JX(config)#lldp start
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#lldp admin-status rx-tx
```

检查配置

使用命令 **show voice-vlan interface** 查看设备的 Voice VLAN 接口状态

```
JX(config)#show voice-vlan interface
  Support max interface      :64
  Current enable interface   :1
  Interface        VID    Mode    Security  RemainTime(s)
-------------------------------------------------------------
  ge-1/0/1         200      auto   enable    N/A
-------------------------------------------------------------
```

2.4 QinQ

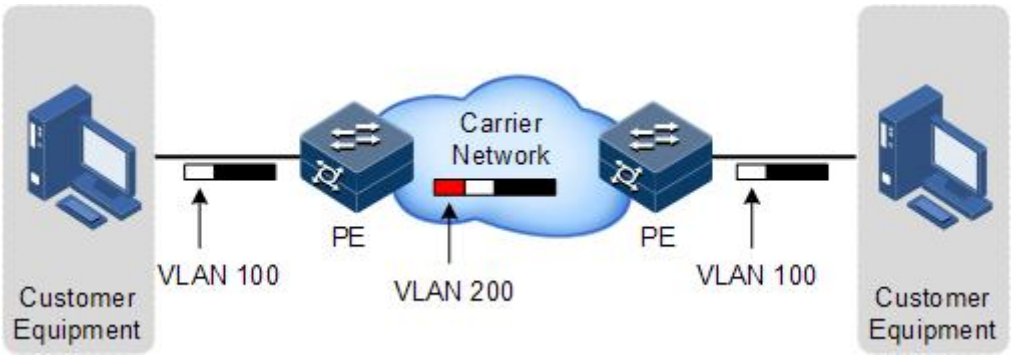
2.4.1 简介

QinQ（也称 Stacked VLAN 或 Double VLAN）技术是对 802.1Q 的扩展，是 IEEE 在 802.1ad 标准中定义的。

基本 QinQ

基本 QinQ 是一种简单的二层 VPN 隧道技术，它通过在运营商接入端为用户的私网报文封装外层 VLAN Tag，使报文携带两层 VLAN Tag 穿越运营商的骨干网络（公网）。在公网中，报文只根据外层 VLAN Tag（即公网 VLAN Tag）进行传输，用户的私网 VLAN Tag 则当作报文中的数据部分来进行传输。

图 2-6 基本 QinQ 典型组网示意图



基本 QinQ 典型组网应用如上图所示，设备作为运营商 PE（Provider Edge）。

报文从用户设备中传送到达 PE 设备，此时报文携带标签的 VLAN ID 为 100。经过 PE 设备用户侧接口时打上外层标签 VLAN 200，经由 PE 设备的网络侧接口进入运营商网络。

带外层标签 VLAN 200 的报文经过运营商传送到达另一端 PE 设备，另一端的 PE 把外层签 VLAN 200 剥去，然后发送到用户设备。报文此时又恢复到只携带一层标签 VLAN 100。

通过该技术可以缓解日益紧缺的公网 VLAN ID 资源，使得用户可以规划自己的私网 VLAN ID，不会导致和公网 VLAN ID 冲突。

灵活 QinQ

灵活 QinQ 是基本 QinQ 的一种增强应用，可以根据一些特性对用户数据进行流分类，然后对不同的类别封装不同的外层 VLAN 标签，它基于接口与 VLAN 结合的方式来实现。除了能实现所有基本 QinQ 的功能外，灵活 QinQ 还能够对同一个接口收到的报文根据不同的 VLAN Tag 做不同的动作，为报文的不同内层 VLAN ID 添加不同的外层 VLAN ID。通过配置内外层 Tag 映射规则，还可以为具有不同内层 Tag 的报文按映射规则封装不同的外层 Tag。也可以将内层优先级复制到外层优先级。

灵活 QinQ 功能可以使运营商的网络构架更为灵活，在连接接入层设备的接口上可以根据 VLAN Tag 对不同的终端用户进行分类，为各类用户封装不同的外层 Tag，并可以在公网中按外层 Tag 配置 QoS 策略，灵活配置数据的传输优先级，使各类用户获得相应的服务。

2.4.2 配置准备

场景

对设备进行基本 QinQ 配置还是灵活 QinQ 配置，需要根据不同的业务需求进行选择。

- 基本 QinQ

通过基本 QinQ 技术应用，用户可以添加外层 VLAN Tag 自由规划自己的私网 VLAN ID，使得运营商网络两端的用户设备之间的数据可以通过运营商网络进行透明输，而不会导致和服务提供商网络中 VLAN ID 冲突。

- 灵活 QinQ

与基本 QinQ 不同，外层 VLAN Tag 是可以根据业务不同进行选择的。用户网络中有多种业务，并设定不同的私网 VLAN ID，针对语音、视频、或数据业务等在运营商网络中通过加不同的外层 VLAN Tag 区分出来，针对不同业务转发的同时实现不同的分流，实现内外层的 VLAN 映射。

前提

在配置 QinQ 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。

- 基本 QinQ 和 1:1VLAN 转换命令行可同时配置，VLAN 转换在基本 QinQ 使能前后功能正常。
- 灵活 QinQ 和 1:1 VLAN 转换命令行可同时配置：同时配置时，灵活 QinQ 和 VLAN 转换功能正常；开启/关闭基本 QinQ，灵活 QinQ 和 VLAN 转换功能正常；取消其中一个配置命令，不影响其他配置正常使用。
- 基本 QinQ、灵活 QinQ 和 2:2VLAN 转换互斥：同时配置灵活 QinQ 和 1:1VLAN 转换时，匹配 VLAN 不能相同，转换后的 VLAN 不能相同。

2.4.3 QinQ 的缺省配置

设备上 QinQ 的缺省配置如下。

功能	缺省值
外层 VLAN Tag 的 TPID 值	0x8100
基本 QinQ 功能状态	禁用
灵活 QinQ 功能状态	禁用

2.4.4 配置基本 QinQ

请在需要的设备的用户侧接口上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。

步骤	配置	说明
3	JX(config-ge-1/0/1)#**port link-type dot1q-tunnel**	使能接口基本 QinQ 功能。
4	JX(config-ge-1/0/1)#**port hybrid pvid** *vlan-id*	配置使能接口的基本 QinQ 功能，添加双层 TAG，指定 CVLAN，SVLAN 使用 PVID。
5	JX(config-ge-1/0/1)#**tpid** *tpid*	配置接口的 VLAN Tag 的 TPID，用于识别用户内层 VLAN 或者 QinQ 使能时识别用户外层 VLAN， tpid：TPID 值，十六进制数，整数形式，取值范围是 0x8100、0x88a8 或 0x9100
6	JX(config-ge-1/0/1)#**inner tpid** *tpid*	配置接口的内层 VLAN Tag 的 TPID，用于识别用户内层 VLAN 或者 QinQ 使能时识别用户外层 VLAN， tpid：TPID 值，十六进制数，整数形式，取值范围是 0x8100、0x88a8 或 0x9100

说明

- 当接口开启基本 QINQ 时，所有报文均当做 Untagged 报文处理，若同时配置 Untagged 报文丢弃，那么 Tagged 的报文也会同时丢弃。

2.4.5 配置灵活 QinQ

请在需要的设备用户侧接口上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-gigaethernet1/0/port)#**vlan-stacking vlan** *vlan-id* **stack-vlan** *vlan-id* **[remark-8021p** *cos-id***]**	配置灵活 qinq 功能。

2.4.6 配置网络侧接口为 Trunk 模式

请在需要配置基本 QinQ 或灵活 QinQ 的设备网络侧接口上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/1)#**port link-type trunk**	配置接口 Trunk 模式，可允许双 Tag 报文通过。

2.4.7 配置 TPID

请在需要设备的网络侧接口进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/1)#**tpid** *tpid*	配置接口的外层 VLAN Tag 的 TPID。

2.4.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show vlan-stacking config**	查看接口基本 QinQ 配置信息。
2	JX#**show vlan-stacking interface**	查看接口的 QinQ 配置信息。
3	JX#**show vlan-stacking resource**	查看 QinQ 的资源信息

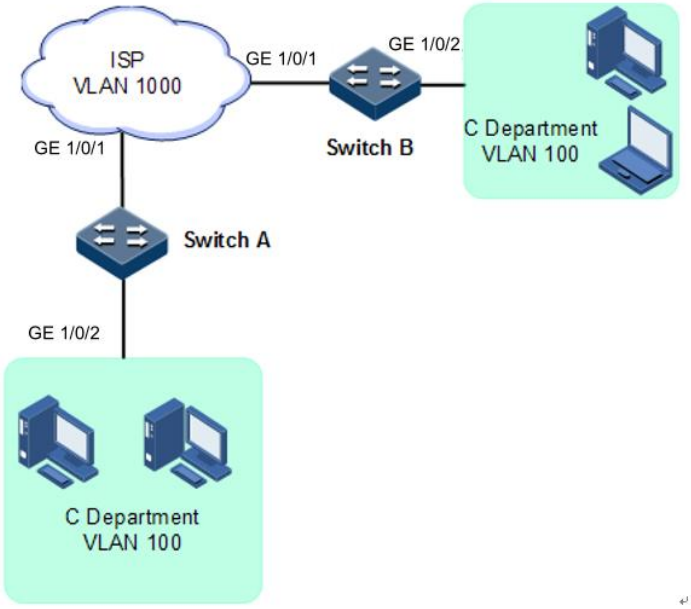
2.4.9 配置基本 QinQ 示例

组网需求

如下图所示，Switch A 和 Switch B 分别连接了 C 部门的 2 个不同地点的网络。C 部门为 VLAN100，要通过运营商 VLAN1000 网络进行通信。运营商的 TPID 为 9100。

通过在 Switch A 和 Switch B 配置基本 QinQ 功能来实现部门内部通过运营商网络的正常通信。

图 2-7 基本 QinQ 应用组网示意图



配置步骤

配置 Switch A 和 Switch B。

Switch A 和 Switch B 配置步骤完全相同，仅以配置 Switch A 为例。

步骤 1 创建 VLAN 100 和 VLAN 1000 并激活。

```
JX#configure
JX(config)#vlan 100,1000
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 1000
JX(config-ge-1/0/1)#tpid 0x9100
JX(config-ge-1/0/1)#exit
```

步骤 2 使能接口的基本 QinQ 功能。

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type dot1q-tunnel
```

```
JX(config-ge-1/0/2)#port default vlan 1000
JX(config-ge-1/0/2)#exit
```

检查结果

通过 **show interface** *interface-type interface-number* **config** 命令查看基本 QinQ 配置信息。

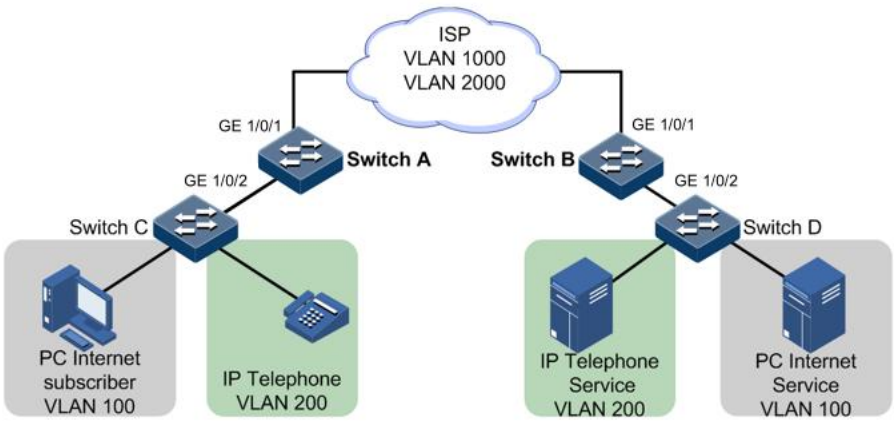
```
JX#show interface ge 1/0/2 config
!
interface ge 1/0/2
 port link-type dot1q-tunnel
 port default vlan 1000
```

2.4.10 配置灵活 QinQ 示例

组网需求

如下图所示，运营商网络区分普通 PC 上网业务和 IP 电话业务，故将 PC 上网业务分配 VLAN 1000，IP 电话业务分配的 VLAN 是 2000。在 Switch A 和 Switch B 上设置灵活 QinQ，将分配给 PC 上网业务的 VLAN 100 添加外层 Tag VLAN 1000，将分配给 IP 电话业务的 VLAN 200 添加外层 Tag VLAN 2000，使用户和服务器间通过运营商的网络能够正常通信。运营商的 TPID 为 9100。

图 2-8 灵活 QinQ 应用组网示意图



配置步骤

配置 Switch A 和 Switch B。

Switch A 和 Switch B 配置步骤完全相同，仅以配置 Switch A 为例。

步骤 1 创建 VLAN 100，200，1000，2000 并激活，TPID 为 9100。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 100,200,1000,2000
```

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 1000,2000
SwitchA(config-ge-1/0/1)#tpid 0x9100
SwitchA(config-ge-1/0/1)#exit
```

步骤 2 使能接口 GE 1/0/2 的灵活 QinQ 功能。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan 100,200,1000,2000
SwitchA(config-ge-1/0/2)#vlan-stacking enable
SwitchA(config-ge-1/0/2)#vlan-stacking vlan 100 stack-vlan 1000
SwitchA(config-ge-1/0/2)#vlan-stacking vlan 200 stack-vlan 2000
SwitchA(config-ge-1/0/2)#exit
```

检查结果

通过 **show vlan-stacking interface** 命令查看灵活 QinQ 配置信息。

以 Switch A 为例。

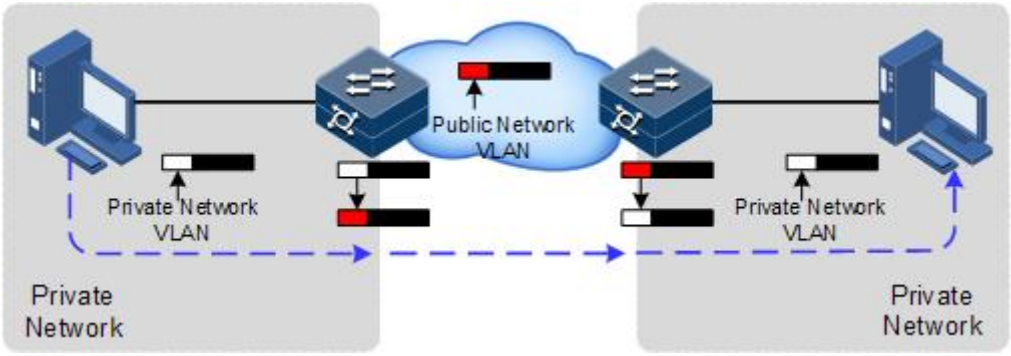
```
SwitchA#show vlan-stacking interface
 Interface         MatchVlan(outer/8021p)
StackVlan(inner/outer/8021p)
--------------------------------------------------------------------------------
-------
 ge-1/0/2          100/-                     -/1000/-
 ge-1/0/2          200/-                     -/2000/-
```

2.5 VLAN 转换

2.5.1 简介

VLAN 转换主要功能是将以太网业务报文中的私网 VLAN Tag 替换为运营商的 VLAN Tag，使其按照运营商的 VLAN 转发规则进行传输。在报文从运营商网络转发到对端用户私网时，再按照同样的规则将 VLAN Tag 恢复为原有的用户私网 VLAN Tag，使报文正确到达目的地。VLAN 转换原理如下图所示。

图 2-9 VLAN 转换原理组网示意图



交换机收到带有用户私网报文的 VLAN Tag 后，根据配置的 VLAN 转换规则对用户私网报文的 VLAN Tag 进行匹配，如果匹配成功，则按照 VLAN 转换规则将私网 VLAN Tag 进行替换。设备支持 1:1 的 VLAN 转换，即将来自某一特定 VLAN 的报文所携带的 VLAN Tag 替换为新的 VLAN Tag。

与 QinQ 功能不同的是，VLAN 转换功能不需要对报文进行多层 VLAN Tag 的封装，只需要更改 VLAN Tag 标记即可，使其按照运营商的 VLAN 转发规则进行传输。

2.5.2 配置准备

场景

与 QinQ 区别的是，VLAN 转换只是变更 VLAN 标签，不额外进行多层 VLAN Tag 的封装，只需要更改 VLAN Tag 标记即可，使其按照运营商的 VLAN 转发规则进行传输，不会增加原报文的帧长度。VLAN 转换可以用在如下场景：

- 用户业务转换为一个运营商的 VLAN ID。
- 多种用户业务转换为一个运营商的 VLAN ID。

前提

在配置 VLAN 转换之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。

2.5.3 VLAN 转换的缺省配置

设备上 VLAN 转换的缺省配置如下。

功能	缺省值
VLAN 转换功能状态	禁止

2.5.4 配置 VLAN 转换

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**vlan-mapping enable**	使能 VLAN 转换功能
4	JX(config-ge-1/0/*)#**vlan-mapping vlan** *vlan-id* **map-vlan** *vlan-id* **[remark-8021p** *cos-id***]**	配置单层 1:1 VLAN 转换规则。
5	JX(config-ge-1/0/*)#**vlan-mapping vlan** *vlan-id* **8021p** *cos-id* **map-vlan** *vlan-id* [**remark-8021p** *cos-id*]	配置单层 1:1 VLAN 匹配 cos 转换规则。
6	JX(config-ge-1/0/*)#**vlan-mapping vlan** *vlan-id* **inner-vlan** *vlan-id* **map-vlan** *vlan-id* **map-inner-vlan** *vlan-id* [**remark-8021p** *cos-id*]	配置内外层 2:2 VLAN 转换规则。
7	JX(config-ge-1/0/*)#**vlan-mapping vlan** *vlan-id* **inner-vlan** *vlan-id* **map-vlan** *vlan-id* [**remark-8021p** *cos-id*]	配置内外层 2:1 VLAN 转换规则。
8	JX(config-ge-1/0/*)#**vlan-mapping 8021p** *vlan-id* **map-vlan** *vlan-id* [**remark-8021p** *cos-id*]	配置匹配 cos 转换规则。

说明

- 基本 QinQ 和 1:1 VLAN 转换命令行可同时配置，VLAN 转换在基本 QinQ 使能前后功能正常。
- 灵活 QinQ 和 1:1 VLAN 转换命令行可同时配置：同时配置时，灵活 QinQ 和 VLAN 转换功能正常；开启/关闭基本 QinQ，灵活 QinQ 和 VLAN 转换功能正常；取消其中一个配置命令，不影响其他配置正常使用。
- 基本 QinQ、灵活 QinQ 和 2:2 VLAN 转换互斥：同时配置灵活 QinQ 和 1:1 VLAN 转换时，匹配 VLAN 不能相同，转换后的 VLAN 不能相同。

2.5.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show vlan-mapping interface**	查看接口的 VLAN 转换规则配置信息。

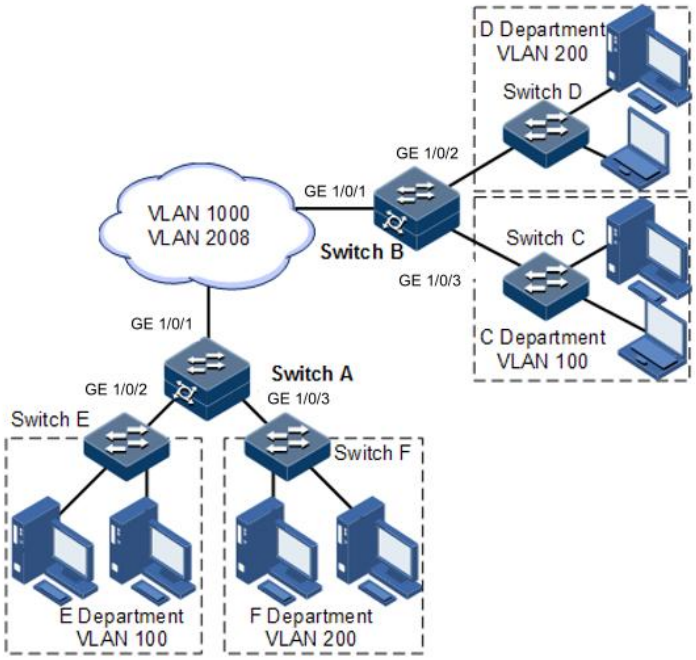
2.5.6 配置 VLAN 转换示例

组网需求

如下图所示，Switch A 的 GE 1/0/2 和 GE 1/0/3 分别连接使用 VLAN 100 的 E 部门和使用 VLAN 200 的 F 部门，Switch B 的 GE 1/0/2 和 GE 1/0/3 分别连接使用 VLAN 100 的 C 部门和使用 VLAN 200 的 D 部门。在运营商网络中为 E 部门和 C 部门分配 VLAN 1000 来传输，为 F 部门和 D 部门分配使用 VLAN 2008 来传输。

通过在 Switch A 和 Switch B 配置 1:1 的 VLAN 转换功能来实现 PC 用户和终端用户与其服务器之间的正常通信。

图 2-10 VLAN 转换应用组网示意图



配置步骤

Switch A 和 Switch B 配置相同，在这里只描述 Switch A 的配置信息。

步骤 1 创建 VLAN 并激活。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 100,200,1000,2008
```

步骤 2 配置接口 GE 1/0/1 为 Trunk 模式，允许 VLAN 1000 和 VLAN 2008 通过。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 1000,2008
SwitchA(config-ge-1/0/1)#exit
```

步骤 3 配置接口 GE 1/0/2 为 Trunk 模式，允许 VLAN 100 通过，配置 VLAN 转换规则。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan 100
SwitchA(config-ge-1/0/2)#vlan-mapping vlan 100 map-vlan 1000
SwitchA(config-ge-1/0/2)#exit
```

步骤 4 配置接口 GE 1/0/3 为 Trunk 模式，允许 VLAN 200 通过，配置 VLAN 转换规则。

```
SwitchA(config)#interface ge 1/0/3
SwitchA(config-ge-1/0/3)#port link-type trunk
SwitchA(config-ge-1/0/3)#port trunk allow-pass vlan 100
SwitchA(config-ge-1/0/3)#vlan-mapping vlan 200 map-vlan 2008
```

检查结果

通过 **show vlan-mapping both interface** 命令查看 1:1 VLAN 转换配置。

```
SwitchA#show vlan-mapping interface
 Interface         MatchVlan(vlan/8021p)        MapVlan(vlan/8021p)
-------------------------------------------------------------------------
--
 ge-1/0/2           inner: -                    inner: -/-
                   outer: 100/-                outer: 1000/-
 ge-1/0/3           inner: -                    inner: -/-
                   outer: 200/-                outer: 2008/-
-------------------------------------------------------------------------
--
```

2.6 MRP/MVRP

2.6.1 简介

MRP（Multiple Registration Protocol，多属性注册协议）作为一个属性注册协议的载体，可以用来传递属性信息。MVRP（Multiple VLAN Registration Protocol，多 VLAN 注册协议）是 MRP 的一种应用，用于在设备间发布并学习 VLAN 配置信息。通过 MVRP，局域网中的设备可以自动同步 VLAN 信息，极大地减少了网络管理员的 VLAN 配置工作。

MRP 消息

MRP 消息主要包括 Join 消息、New 消息、Leave 消息和 LeaveAll 消息

- Join 消息：当一个 MRP 实体配置了某些属性，需要对端实体来注册自己的属性信息时，它会向对端实体发送 Join 消息。当一个 MRP 实体收到来自对端实体的 Join 消息时，它会注册该 Join 消息中的属性，并向本设备的其他实体传播该 Join 消息，其他实体收到传播的 Join 消息后，向其对端实体发送 Join 消息。
- New 消息：New 消息的作用和 Join 消息比较类似，都是用于对属性的声明。不同的是，New 消息主要用于 MSTP（Multiple Spanning Tree Protocol，多生成树协议）拓扑变化的情况。

- Leave 消息：当一个 MRP 实体注销了某些属性，需要对端实体进行同步注销时，它会向对端实体发送 Leave 消息。当一个 MRP 实体收到来自对端实体的 Leave 消息时，它会注销该 Leave 消息中的属性，并向本设备的其他实体传播该 Leave 消息，其他实体收到传播的 Leave 消息后，根据该 Leave 消息中的属性在本设备上的状态，决定是否向其对端实体发送该 Leave 消息（比如该 Leave 消息中的属性为某 VLAN，若该 VLAN 为动态 VLAN，且本设备上无实体注册该 VLAN，则在设备上删除该 VLAN，并向对端实体发送该 Leave 消息；若该 VLAN 为静态 VLAN，则不向对端实体发送该 Leave 消息）。
- LeaveAll 消息：每个 MRP 实体启动时都会启动各自的 LeaveAll 定时器，当该定时器超时后，MRP 实体就会向对端实体发送 LeaveAll 消息。当一个 MRP 实体收发 LeaveAll 消息时，它会启动 Leave 定时器，同时根据自身的属性状态决定是否发送 Join 消息要求对端实体重新注册某属性。该实体在 Leave 定时器超时前，重新注册收到的来自对端实体的 Join 消息中的属性；在 Leave 定时器超时后，注销所有未重新注册的属性信息，从而周期性地清除网络中的垃圾属性。

Leave 消息、LeaveAll 消息通过与 Join 消息配合，确保属性的注销或重新注册。通过消息交互，所有待注册的属性信息可以传播到同一局域网内使能 GARP 功能的所有设备上。

MRP 定时器

MRP 消息发送的时间间隔通过定时器来实现，MRP 定义了四种定时器，用于控制 MRP 消息的发送周期。

- Periodic 定时器：每个 MRP 实体启动时都会启动各自的 Periodic 定时器，来控制 MRP 消息的周期发送。该定时器超时前，实体收集需要发送的 MRP 消息，在该定时器超时后，将所有待发送的 MRP 消息封装成尽可能少的报文发送出去，这样减少了报文发送数量。随后再重新启动 Periodic 定时器，开始新一轮的循环。
- Join 定时器：用来控制 Join 消息的发送。为了保证消息能够可靠地发送到对端实体，MRP 实体在发送 Join 消息时，将启动 Join 定时器。如果在该定时器超时前收到了来自对端实体的 JoinIn 消息，且该 JoinIn 消息中的属性与发出的 Join 消息中的属性一致，便不再重发该 Join 消息，否则在该定时器超时后，当 Periodic 定时器也超时，它将重发一次该 Join 消息。
- Leave 定时器：用来控制属性的注销。当 MRP 实体收到来自对端实体的 Leave 消息（或收发 LeaveAll 消息）时，将启动 Leave 定时器。如果在该定时器超时前，收到来自对端实体的 Join 消息，且该 Join 消息中的属性与收到的 Leave 消息中的属性一致（或与收发的 LeaveAll 消息中的某些属性一致），则这些属性不会在本实体被注销，其他属性则会在该定时器超时后被注销。
- LeaveAll 定时器：每个 MRP 实体启动时都会启动各自的 LeaveAll 定时器，当该定时器超时后，该实体就会向对端实体发送 LeaveAll 消息，随后再重新启动 LeaveAll 定时器，开始新一轮的循环，对端实体在收到 LeaveAll 消息后也重新启动 LeaveAll 定时器。

MVRP

MVRP（Multiple VLAN Registration Protocol，多 VLAN 注册协议）是 MRP 的一种应用，它基于 MRP 的工作机制，维护交换机中的 VLAN 动态注册信息，并传播该信息到其它交换机。

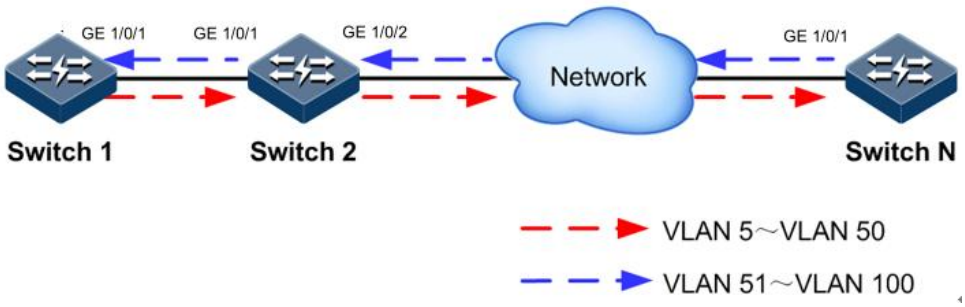
所有支持 MVRP 特性的交换机能够接收来自其它交换机的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息。而且所有支持 MVRP 特性的交换机能够将本地的 VLAN 注册信息向其它交换机传播，以便使同一交换网内所有支持 MVRP 特性的设备 VLAN 信息达成一致。MVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它交换机的动态注册信息。

MVRP 有三种注册模式：

- 正常模式（Normal）：允许动态注册、注销 VLAN，传播动态、静态 VLAN 信息。
- 固定模式（Fixed）：禁止动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息，只允许静态 VLAN 通过，即只对其他 MVRP 成员传播静态 VLAN 信息。
- 禁止模式（Forbidden）：禁止动态注册、注销 VLAN，禁止静态 VLAN 在接口上的创建，同时删除接口上除 VLAN 1 外的所有 VLAN，只允许缺省 VLAN（即 VLAN 1）通过，只对其他 MVRP 成员传播缺省 VLAN 的信息。

存在多台设备的网络中，如图 2-11 所示，如果想在每台设备上配置 VLAN 信息，并允许指定 VLAN 的报文通过是比较繁琐的。采用 MVRP 来动态注册和传播指定 VLAN，可以帮助网管人员提高工作效率，提高准确性。

图 2-11 MVRP 原理示意图



在图 2-11 中，Switch 1 的 GE 1/0/1，Switch 2 的 GE 1/0/1 和 GE 1/0/2，Switch N 的 GE 1/0/1 均为 Trunk 接口。在 Switch 1 中创建 VLAN 5～VLAN 50，则会按照红色连接线方向在接收接口上动态注册该 VLAN，直到传播到 Switch N 交换机。在 Switch N 上创建 VLAN 51～VLAN 100，则沿蓝色连接线注册该 VLAN 信息，使每个交换机可以完全处理 VLAN 5～VLAN 100 的报文。

2.6.2 配置准备

场景

利用 MVRP 机制，一个 MVRP 成员上的配置信息会迅速传播到整个局域网中所有使能 MVRP 功能的设备上。

通过 MVRP 功能配置的 Join 定时器、Leave 定时器和 LeaveAll 定时器的值，将应用于所有在同一网络内运行的 MVRP 应用。

前提

无

2.6.3 缺省配置

MVRP 缺省配置

设备上 MVRP 的缺省配置如下

功能	缺省值
全局 MVRP 功能状态	禁止
接口 MVRP 功能状态	禁止
MVRP 注册模式	Normal

2.6.4 配置 MVRP 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**mvrp start**	使能全局 MVRP 功能。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
4	JX(config-ge-1/0/1)#**port link-type trunk**	配置接口为 Trunk 模式。
5	JX(config-ge-1/0/1)#**mvrp registration** { **fixed** | **forbidden** | **normal** }	配置 MVRP 注册模式。
6	JX(config-ge-1/0/1)#**mvrp enable**	使能接口 MVRP 功能。

注意

- 接口必须先配置为 Trunk 模式才能使能接口 MVRP 功能。
- 不建议用户在聚合组成员接口上使能 MVRP 功能。

2.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show mvrp config**	查看 MVRP 的配置信息。
2	JX#**show mvrp**	查看 MVRP 的接口状态信息。
3	JX#**show mvrp interface** *interface-type interface-number* **vlan** *vlan-id*	查看 MVRP 的定时器信息。

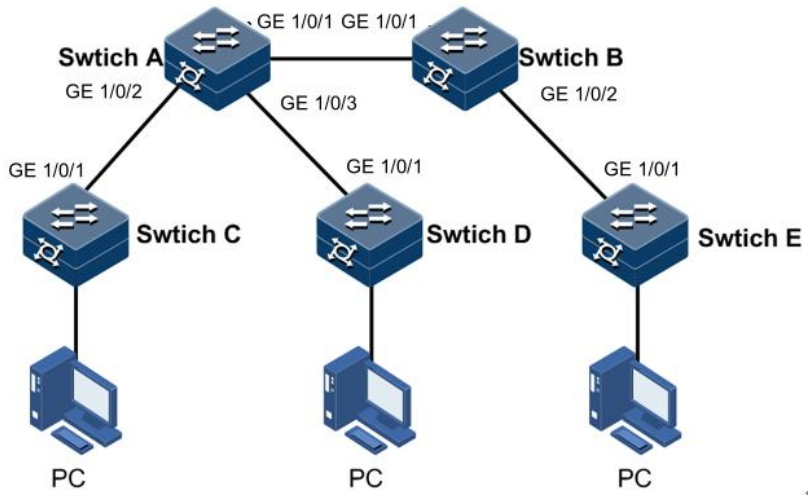
2.6.6 配置 MVRP 应用示例

组网需求

为了在交换机之间动态注册和更新 VLAN 信息，如图 2-12 所示，需要在各交换机上配置 MVRP 功能，来实现各交换机设备之间 VLAN 信息的动态注册和注销。具体要求如下：

- 在 Switch A 和 Switch C 中配置静态 VLAN 5～VLAN 10。
- Switch D 中配置静态 VLAN 15～VLAN 20。
- Switch E 中配置静态 VLAN 25～VLAN 30。
- 将所有与其他交换机相连的接口设置为 Trunk 模式，然后使能接口的 MVRP 功能。
- 配置各接口 MVRP 的 Join 定时器、Leave 定时器和 LeaveAll 定时器分别为 3000、15000 和 20000。

图 2-12 MVRP 应用组网示意图



配置步骤

步骤 1 创建 VLAN 并使能全局 MVRP 功能。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 5-10
SwitchA(config)#mvrp start
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#configure
SwitchB(config)#mvrp start
```

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#configure
SwitchC(config)#vlan 5-10
SwitchC(config)#mvrp start
```

配置 Switch D。

```
JX#hostname SwitchD
SwitchD#config
SwitchD(config)#vlan 15-20
SwitchD(config)#mvrp start
```

配置 Switch E。

```
JX#hostname SwitchE
SwitchE#configure
SwitchE(config)#vlan 25-30
SwitchE(config)#mvrp start
```

步骤 2 分别配置 Switch A 的 GE 1/0/1、GE 1/0/2、GE 1/0/3 接口，Switch B 的 GE 1/0/1、GE 1/0/2，Switch C 的 GE 1/0/1，Switch D 的 GE 1/0/1 接口为 Trunk 模式，并使能接口的 MVRP 功能。以配置 Switch A 的 GE 1/0/1 接口为例，其余接口配置步骤相同。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/1)#mvrp enable
SwitchA(config-ge-1/0/1)#exit
```

步骤 3 分别配置 Switch A 的 GE 1/0/1、GE 1/0/2、GE 1/0/3 接口、Switch B 的 GE 1/0/1、GE 1/0/2，Switch C 的 GE 1/0/1，Switch D 的 GE 1/0/1 接口的 GARP 定时器时间。以配置 Switch A 为例，其余接口配置步骤相同。

配置 Switch A。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#mvrp timer join 3000
SwitchA(config-ge-1/0/1)#mvrp timer leave 15000
SwitchA(config-ge-1/0/1)#mvrp timer leave-all 20000
```

检查结果

通过 **show mvrp** 命令查看设备上接口的 MVRP 配置信息，以 Switch A 为例。

```
SwitchA#show mvrp
```

```
 Version              : MVRP_v13.10.00.00

 Compliance-GVRP       : disable

 Interface        JoinTime(ms)    LeaveTime(ms)   LeaveAllTime(ms)
PeriodicTime(ms)  Mode     State

--------------------------------------------------------------------------
--------------------------------

GE 1/0/1         3000          15000         20000          --
normal    enable
```

通过 **show vlan** 命令查看设备上的 VLAN 信息，以 Switch A 为例。

```
SwitchA#show vlan

NOTE:

    S: supervlan       P: pvlan        N: normal


 Vlan  Type       Ports('M': member , '-': not member)

--------------------------------------------------------------------------
-------

 1    N/static    untagged: ge-1/0/1<->ge-1/0/16          MMMMMMMM
MMMMMMMM

                        ge-1/0/17<->ge-1/0/32          MMMMMMMM MMMMMMMM

                        ge-1/0/33<->ge-1/0/48          MMMMMMMM MMMMMMMM

                        10ge-1/0/49<->10ge-1/0/54      MMMMMM

 2    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 3    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 4    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 5    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 6    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 7    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 8    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 9    N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 10   N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

 20   N/mvrp     tagged:   ge-1/0/1<->ge-1/0/16          M------- --------

--------------------------------------------------------------------------
-------

  Total: 11   Static: 1   Dynamic: 10
```

3 IP 业务

本章介绍 IP 业务特性的基本原理和配置过程，并提供相关的配置案例。

- IP 基础配置
- LOOPBACK 接口
- ARP
- NDP
- 静态路由
- 策略路由

3.1 IP 基础配置

3.1.1 简介

IP 接口是基于 VLAN 的虚拟接口。一般应用于需要对设备进行网管或多台设备之间需要进行路由连通的场合。

设备支持管理 VLAN 报文为双 TAG，能够发送和处理双 TAG 报文。

3.1.2 配置准备

场景

为每一个 VLAN 接口、SNMP 或 LOOPBACK 接口配置 IP 地址。

前提

为 VLAN 接口配置 IP 地址前，需创建 VLAN 并激活。

3.1.3 VLAN 接口的缺省配置

设备上 VLAN 接口的缺省配置如下。

功能	缺省值
管理 VLAN 内层 TPID	0x8100
管理 VLAN 内层 VLAN	1
SNMP 接口 IP 地址	192.168.0.1

3.1.4 配置 VLAN 接口 IPv4 地址

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	创建 VLAN。
3	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
4	JX(config-vlanif-*)#**ip address** *ip-address* [*ip-mask*]	配置 VLAN 接口的主 IP 地址。 可以使用 **no ip address** *ip-address* 命令删除主 IP 地址配置。
5	JX(config-vlanif-*)#**ip address** *ip-address* [*ip-mask*] **sub**	配置接口的从 IP 地址。 可以使用 **no ip address** *ip-address* 命令删除从 IP 地址配置。

3.1.5 配置 VLAN 接口 IPv6 地址

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	创建 VLAN。
3	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
4	JX(config-vlanif-*)#**ipv6 enable**	配置 VLAN 接口 IPv6 使能。
5	JX(config-vlanif-*)#**ipv6 address** ipv6-address/prefix-length JX(config-vlanif-*)#**ipv6 address** ipv6-address **link-local**	配置 VLAN 接口的 IPv6 地址。
6	JX(config-vlanif-*)#**ipv6 address auto global**	配置 VLANIF 接口的 IPv6 无状态自动生成 IPv6 全局地址功能使能

3.1.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

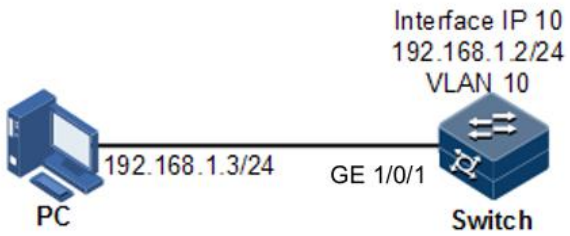
序号	检查项	说明
1	JX#show ip interface	查看 VLAN 接口的 IP 地址配置信息。
2	JX#show ipv6 interface	查看 VLAN 接口的 IPv6 地址配置信息。

3.1.7 配置 VLAN 接口 IP 地址实现和主机互通示例

组网需求

配置交换机设备 VLAN 接口，使图 3-1 中的主机和设备之间能够相互 Ping 通。

图 3-1 配置 VLAN 接口组网示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#config
JX(config)#vlan 10
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port hybrid pvid 10
JX(config-ge-1/0/1)#port hybrid vlan 10 untagged
JX(config-ge-1/0/1)#quit
```

步骤 2 在交换机设备上创建三层接口，配置三层接口的 IP 地址并关联 VLAN。

```
JX(config)#interface vlan 10
JX(config-vlan10)#ip address 192.168.1.2 255.255.255.0
```

检查结果

通过 **show vlan** 命令查看 VLAN 和物理接口的绑定关系是否正确。

```
JX#show vlan 10
```

```
vlan-10 information:
------------------------------------------------------------
  Description                :
  Admin state                : up
  Operation state             : down
  Vlan type                  : normal
  Vlan status                : static
  Unknown multicast state      : forward
  Unknown unicast state        : forward
  IPv4 address total number     : 0
  IPv6 address total number     : 0

  Ports :
    Interface                 Tagged
    ------------------------------------
    ge-1/0/1                  Untag
------------------------------------------------------------
```

通过 **show ip interface** 命令查看三层接口配置是否正确。

```
JX#show ip interface
 Total number: 2
 Interface         State(a/o) Addr/Prefix       Role     Type      Vpn-
instance
------------------------------------------------------------------------------
---------------------------
 loopback-0         up/up     127.0.0.1/8       primary   auto      N/A
 vlan-10           up/up    192.168.1.2/24    primary   static    N/A
------------------------------------------------------------------------------
---------------------------
```

通过 **ping** 命令查看设备和 PC 之间是否能够互通。

```
JX#ping 192.168.1.3
PING 192.168.1.3: 64 data bytes
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=1
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=2
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=3
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=4
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=5
PING Statistics for 192.168.1.3
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

3.2 LOOPBACK 接口

3.2.1 简介

LOOPBACK 接口是一种虚拟接口，可以分为两类：

- 由系统自动创建的 LOOPBACK 接口。IP 地址固定为 127.0.0.1，用来接收所有发送给本机的数据包。不通过路由协议对外发布。

- 由用户创建的 LOOPBACK 接口。在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口，并且接口状态永远是 up 状态，能够被路由协议发布出去。

LOOPBACK 接口状态不受物理接口 Up/Down 的影响，只要保证设备运行正常，该 LOOPBACK 接口就不会 Down 掉。因此，LOOPBACK 接口地址常被用来标示物理设备本身，作为设备的管理地址。

3.2.2 配置准备

场景

使用 LOOPBACK 接口 IP 地址对设备进行 Telnet 登录，可以保证 Telnet 操作不会因接口的物理状态改变为 Down 掉，如果 PC 需要 ping 通 LOOPBACK 接口地址，需要 PC 端设置相对应的静态路由表项。LOOPBACK 接口还常被用来作为动态路由协议如 OSPF 等协议的 Router ID，作为设备的唯一标识。

前提

无

3.2.3 LOOPBACK 接口的缺省配置

无

3.2.4 配置 LOOPBACK 接口 IP 地址

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface loopback** *loopback-number*	进入 LOOPBACK 接口配置模式。
3	JX(config-loopback-*)#**ip address** *ip-address* [*ip-mask*] [**sub**]	配置 LOOPBACK 接口的 IP 地址。
4	JX(config-loopback-*)#**ipv6 enable**	配置 LOOPBACK 接口 IPv6 使能。
4	JX(config-loopback*)#**ipv6 address** ipv6-address/prefix-length JX(config-loopback-*)#**ipv6 address** ipv6-address **link-local**	配置 LOOPBACK 接口的 IPV6 地址。

3.2.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show interface loopback** [*loopback-number*]	查看 LOOPBACK 接口配置信息。

3.3 SLAAC

3.3.1 简介

无状态地址自动配置（Stateless Address Autoconfiguration,SLAAC）是 IPv6 节点（主机或路由器）用于为接口自动配置 IPv6 地址的过程。无状态地址自动配置会自动执行某些网络管理员的任务。

3.3.2 配置准备

场景

节点通过将地址前缀与节点的 MAC 地址派生的标识或用户指定的接口标识组合来构建各种 IPv6 地址。这些前缀包括本地链路前缀（fe80::/10）和本地 IPv6 路由器（如果存在）所通告的长度为 64 的前缀。

前提

无

3.3.3 SLAAC 的缺省配置

功能	缺省值
无状态地址自动配置	去使能

3.3.4 使能 SLAAC

步骤	配置	说明
1	JX(config)#**interface vlan** *vlan-id*	进入 VLANIF 配置模式。
2	JX(config-vlanif-*)#**ipv6 address auto global**	使能无状态地址自动配置。

3.3.5 配置 SLAAC 示例

使能设备无状态地址自动配置

```
JX(config-vlanif-*)#ipv6 enable
JX(config-vlanif-*)#ipv6 address auto global
```

3.4 ARP

3.4.1 简介

在 TCP/IP 网络环境中，每台主机都被分配了一个 32 位的 IP 地址，这种互联网地址是在网际范围内标识主机的一种逻辑地址。为了让报文在物理链路中传送，必须知道目的主机的物理地址。这就需要把 IP 地址通过映射关系转换成物理地址。在以太网环境中采用的物理地址是 48 位 MAC 地址，为了正确地向目的主机传送报文，必须把目的主机的 32 位 IP 地址转换成为 48 位以太网的地址。为此产生了 ARP（Address Resolution Protocol，地址解析协议），该协议主要用于 IP 地址到 MAC 地址的解析，建立 IP 地址和 MAC 地址的映射关系。

ARP 地址映射表项包括以下两种类型：

- 静态表项：静态表项是将 IP 地址和 MAC 地址进行静态绑定，用于防止 ARP 动态学习欺骗。
  - 静态 ARP 地址表项需要手动添加，手动删除。
  - 静态 ARP 地址不老化。
- 动态表项：设备通过 ARP 协议自动学习到的 MAC 地址。
  - 动态表项生成由交换机自动完成，不需要手动配置，可以调整动态 ARP 的一些参数。
  - 如果不使用，到达老化时间会老化。

3.4.2 配置准备

场景

IP 地址和 MAC 地址的映射关系保存在 ARP 地址映射表中。

一般情况下，ARP 地址映射表项由设备动态维护，设备按照 ARP 协议自动寻找 IP 地址和 MAC 地址之间的映射关系，无需用户关注。只有在防止 ARP 动态学习欺骗，需要添加静态 ARP 地址映射表项时，才需要对设备进行手动配置。

前提

无

3.4.3 ARP 的缺省配置

设备上 ARP 的缺省配置如下。

功能	缺省值
静态 ARP 表项	无
动态 ARP 老化时间	1200 秒

3.4.4 配置静态 ARP 表项

注意

- 静态添加的 ARP 表项的 IP 地址必须属于交换机三层接口所属的 IP 网段。
- 静态 ARP 表项，需要手动添加和手动删除。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**arp static** *ip-address mac-address* { **ge | 10ge** } *interface-number*	配置静态 ARP 表项。

3.4.5 配置动态 ARP 表项

请在需要配置的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
3	JX(config)#**arp aging-time {** *aging-time* | *default* **}**	配置动态 ARP 老化时间。

3.4.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show arp**	查看 ARP 地址映射表中的表项信息。

3.4.7 维护

用户可以通过以下命令，维护设备 ARP 特性的运行情况和配置情况。

命令	描述
JX(config)#**flush arp** [*all* | *dynamic*| *static*]	清空 ARP 地址映射表中表项。

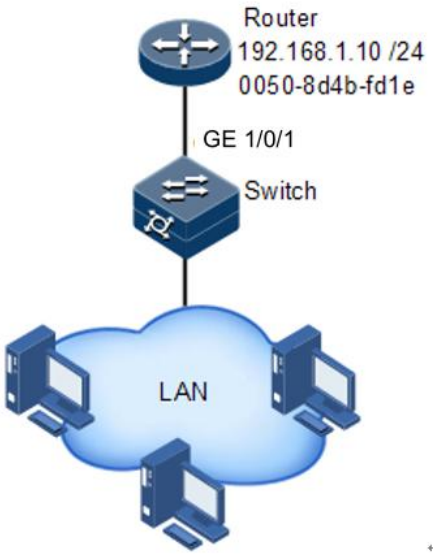
3.4.8 配置 ARP 示例

组网需求

如图 3-2 所示，交换机设备连接主机，通过接口 GE 1/0/1 连接上游的 Router。Router 的 IP 地址为 192.168.1.10/24，MAC 地址为 0050.8d4b.fd1e。

为了增加交换机和 Router 通信的安全性，需要在交换机上配置相应的静态 ARP 表项。

图 3-2 配置 ARP 组网示意图



配置步骤

创建 VLAN3。

```
JX#configure
JX(config)#vlan 3
```

将接口 GE1/0/1 加入 VLAN3 中。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port hybrid pvid 3
JX(config-ge-1/0/1)#port hybrid vlan 3 untagged
JX(config-ge-1/0/1)#quit
```

创建接口 VLANIF3。

```
JX(config)#interface vlan 3
```

配置接口 VLANIF3 的 IP 地址。

```
JX(config-vlanif-3)#ip address 192.168.1.1/24
JX(config-vlanif-3)#quit
```

配置增加一条 ARP 静态表项。

```
JX#configure
JX(config)#arp static 192.168.1.10 00:50:8d:4b:fd:1e ge 1/0/1
```

检查结果

通过 **show arp** 命令查看 ARP 地址映射表中的所有表项信息是否正确。

```
JX#show arp
Arp aging time: 1200(s)
Arp entry types: D-Dynamic, S-Static, I-Interface, DH-Dhcp, B-Bgp, INV-
Invalid

IP-addr    Mac-addr   Type Aging   Vlan(O/I)   Interface         Vpn-
instance

------------------------------------------------------------------------------
----------------------------------

192.168.1.1    0002:5600:0001  I    -      -/-          vlan-3
N/A

192.168.1.10    0050:8d4b:fd1e   S    -      3/-          ge-1/0/1
N/A

------------------------------------------------------------------------------
----------------------------------

Total: 2       Dynamic: 0       Static: 1       Bgp: 0       Other: 1
```

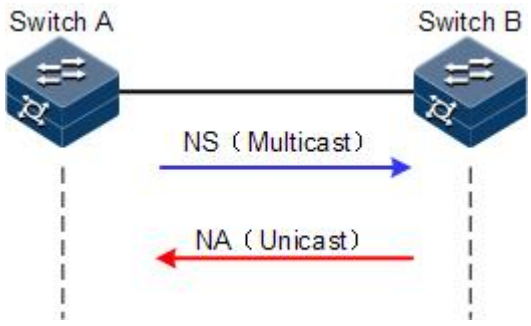
3.5 NDP

3.5.1 简介

NDP（Neighbor Discovery Protocol，邻居发现协议）通过在同一链路上的 IPv6 设备上使用邻居发现机制，来发现彼此的存在、确定彼此的 MAC 地址并维护邻居设备信息。

NDP 通过邻居请求消息 NS（Neighbor Solicitation）和邻居通告消息 NA（Neighbor Advertisement）获取同一链路上邻居设备的链路层地址，即 MAC 地址。

图 3-3 NDP 地址解析原理示意图



如图 3-3 所示，以 Switch A 为例，Switch A 要获取 Switch B 的链路层地址。具体报文处理过程如下：

1. Switch A 通过组播方式发送 NS 消息。其中 NS 消息的源地址是 Switch AVLAN 接口的 IPv6 地址，目的地址是 Switch B 的被请求节点组播地址，消息内容中还包含了 Switch A 的链路层 MAC 地址。

2. Switch B 收到 NS 消息后，判断报文的目的地址是否为自己的 IPv6 地址对应的被请求设备组播地址。如果是，则 Switch B 可以学习到 Switch A 的链路层地址，并以单播方式发送 NA 消息，其中包含了自身的链路层地址。

3. Switch A 收到 Switch B 发送的 NA 消息，就可以获得 Switch B 的链路层地址。

IPv6 邻居发现协议通过使用 ICMPv6 消息，还可以实现验证邻居是否可达、重复地址检测、路由设备发现/前缀发现、地址自动配置和重定向等功能。

3.5.2 配置准备

场景

IPv6 邻居发现协议不但实现了 IPv4 中的 ARP 协议、ICMP 重定向和 ICMP 设备发现等功能，还提供了邻居可达性检测功能。

前提

在配置 NDP 功能之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 配置 VLAN 接口的 IPv6 地址。

3.5.3 NDP 的缺省配置

设备上 NDP 的缺省配置如下。

功能	缺省值
动态 NDP 老化时间	1200 秒

3.5.4 配置静态邻居表项

将邻居节点的 IPv6 地址解析为链路层地址，可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态实现，也可以通过手工配置静态邻居表项来实现。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#configure	进入全局配置模式。

步骤	配置	说明
2	JX(config-vlanif-*)#**ipv6 neighbor** *ipv6-address mac-address* { **ge | 10ge** } *interface-number*	配置静态邻居表项信息。

3.5.5 配置动态 NDP 老化时间

邻居信息表项中的表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将从邻居信息表项中删除，这个生存周期被称作老化时间。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**ipv6 nd lifetime** { *aging-time* | *default* }	配置动态 NDP 老化时间。

3.5.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show ipv6 neighbor**	查看所有 NDP 邻居信息。

3.5.7 维护

用户可以通过以下命令维护 NDP 特性。

命令	描述
JX(config)#**flush ipv6 neighbor** [*all* | *dynamic*| *static*]	清除所有 IPv6 邻居信息。

3.6 静态路由

3.6.1 简介

路由是将报文穿过网络传递到目的地的行为，在传递过程中采用路由表进行转发。不同 VLAN 间的设备进行通讯，或同一 VLAN 跨越不同网络进行通信，需要使用路由功能。

缺省路由

缺省路由是一种特殊的静态路由，只有在路由表中没有找到匹配的路由表项时才会被使用。在路由表中，缺省路由以到达网络 IP 地址 0.0.0.0、掩码为 0.0.0.0 的路由形式出现。可通过命令 **show ip route** 查看当前是否配置了缺省路由。如果设备没有配置缺省路由且报文的目的 IP 地址不在路由表中，那么设备在丢弃该报文的同时，会向报文发送端返回一个 ICMP 报文，报告该目的地址或网络不可达。

静态路由

静态路由是需要用户手动配置的路由，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。缺点是不能自动适应网络拓扑的变化，需要人工干预。

3.6.2 配置准备

场景

对于拓扑结构比较简单的网络，可以配置静态路由。静态路需要由用户手动配置，通过配置静态路由可以建立一个互通的网络。

前提

正确配置 VLAN 接口的 IP 地址。

3.6.3 配置静态路由

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**ip route-static** *ip-address mask-address nexthop-address* [**preference** *preferencevalue*]	配置 IPv4 静态路由。
	JX(config)#**ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address* [**preference** *preference-value*]	配置 IPv6 静态路由。

3.6.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

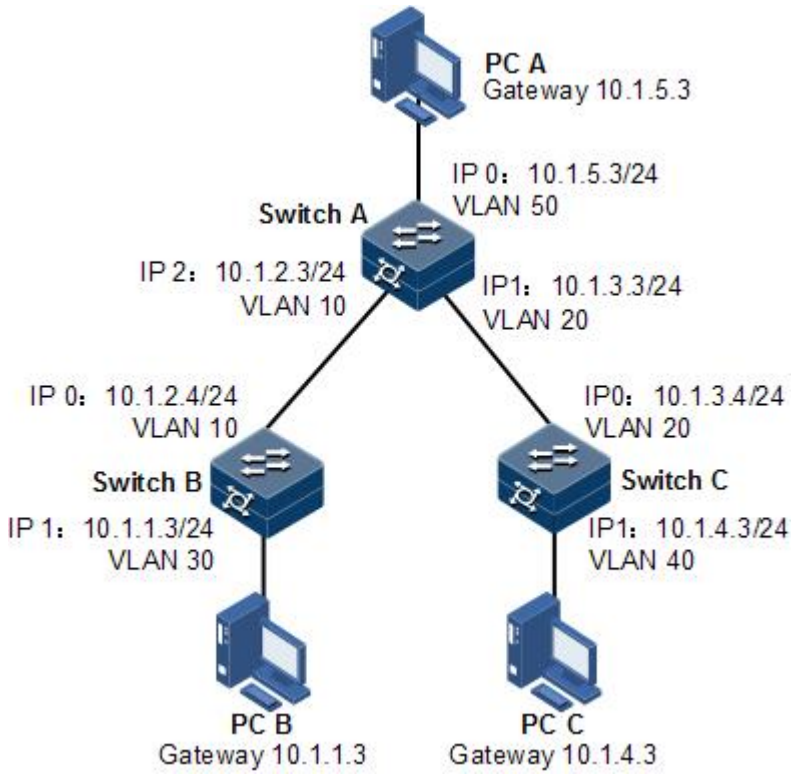
序号	检查项	说明
1	JX#**show ip route**	查看路由表信息。
	JX#**show ipv6 route**	
2	JX#**show { ip | ipv6 } route statistics**	查看路由统计信息。

3.6.5 配置静态路由示例

组网需求

配置静态路由，使图 3-4 中的任意两台主机或交换机设备之间能够相互 Ping 通。

图 3-4 配置静态路由组网示意图



配置步骤

步骤 1 配置各设备的 IP 地址。具体配置略。

步骤 2 在 Switch A 上配置静态路由。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#ip route-static 10.1.1.0 255.255.255.0 10.1.2.4
SwitchA(config)#ip route-static 10.1.4.0 255.255.255.0 10.1.3.4
```

步骤 3 在 Switch B 上配置缺省网关。

```
JX#hostname SwitchB
SwitchB#configure
SwitchB(config)#ip route-static 0.0.0.0 0.0.0.0 10.1.2.3
```

步骤 4 在 Switch C 上配置缺省网关。

```
JX#hostname SwitchC
SwitchC#configure
SwitchC(config)#ip route-static 0.0.0.0 0.0.0.0 10.1.3.3
```

步骤 5 在主机 A 上配置默认网关为 10.1.5.3，具体配置略。

步骤 6 在主机 B 上配置默认网关为 10.1.1.3，具体配置略。

步骤 7 在主机 C 上配置默认网关为 10.1.4.3，具体配置略。

检查结果

通过 **ping** 命令查看所有设备之间是否均能两两互通。

```
SwitchA#ping 10.1.1.3
PING 10.1.1.3: 64 data bytes
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=1
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=2
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=3
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=4
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=5
PING Statistics for 10.1.1.3
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

3.7 策略路由

3.7.1 简介

概述

传统上，普通的报文转发是依据报文的目的地址查询转发表来实现的，当遇到需要根据源 IP 来控制报文转发，根据报文的长度来控制报文转发或根据报文的其他属性来控制报文转发时，就需要一种新的路由机制来控制，也就是策略路由来控制。

所谓策略路由，顾名思义，即是根据一定的策略进行报文转发，因此策略路由是一种比目的路由更灵活的路由机制。在路由器转发一个数据报文时，首先根据配置的规则对报文进行过滤，匹配成功则按照一定的转发策略进行报文转发。这种规则可以是基于标准和扩展访问控制列表，也可以基于报文的长度；而转发策略则是控制报文按照

指定的策略路由表进行转发，也可以修改报文的 IP 优先字段。因此，策略路由是对传统 IP 路由机制的有效增强。

技术介绍

策略路由能满足基于源 IP 地址、目的 IP 址、协议字段，甚至于 TCP、UDP 的源、目的端口等多种组合进行选路。简单点来说，只要 IP standard/extended ACL 能设置的，都可以做为策略路由的匹配规则进行转发。

策略路由（Policy Route）在决定一个 IP 包的下一跳转发地址或是下一跳缺省 IP 地址时，不是简单的根据目的 IP 地址决定，而是综合考虑多种因素来决定。如可以根据 DSCP（差分服务代码点）字段、源和目的端口号，源 IP 地址等来为数据包选择路径。策略路由可以在一定程度上实现流量工程，使不同服务质量的流或者不同性质的数据（语音、FTP）走不同的路径。

基于策略的路由为网络管理者提供了比传统路由协议对报文的转发和存储更强的控制能力。传统上，路由器用从路由协议派生出来的路由表，根据目的地址进行报文的转发。基于策略的路由比传统路由能力更强，使用更灵活，它使网络管理者不仅能够根据目的地址而且能够根据协议类型、报文大小、应用或 I P 源地址来选择转发路径。策略可以定义为通过多路由器的负载平衡或根据总流量在各线上进行报文转发的服务质量（Q o S ）。

策略路由功能的实现是依靠芯片的支持，策略路由功能是通过命令行或其它配置界面，将软件表项转换为硬件表项存储到芯片上去，当流量通过时，芯片会按照策略路由硬件表来过滤报。

3.7.2 配置准备

场景

策略路由能满足基于源 IP 地址、目的 IP 址、协议字段，甚至于 TCP、UDP 的源、目的端口等多种组合进行选路。

前提

正确配置 VLAN 接口的 IP 地址，ACL。

3.7.3 配置策略路由

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**policy-route** *NAME* { **permit** | **deny** } **node** *node-id*	创建策略路由模板。
3	JX(config-policy-route-xxx-1)#**if-match acl-ipv4** *acl-ipv4-number*	设置 ACL 的匹配规则。

步骤	配置	说明
4	JX(config-policy-route-xxx-1)#**apply ip-address next-hop** *ip-address*	设置报文的下一跳
5	JX(config-ge-xxx)#**policy-route bind-policy** *NAME*	将策略路由应用到物理端口

3.7.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

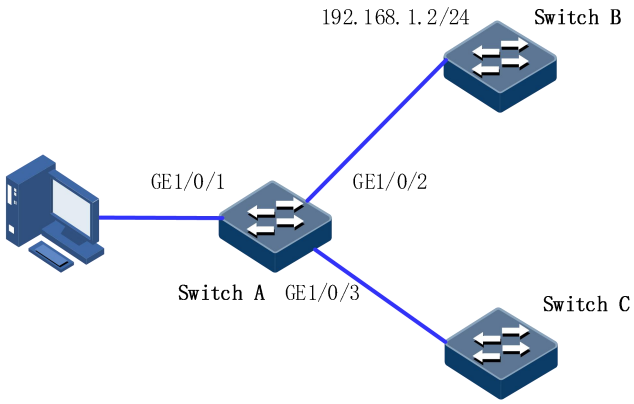
序号	检查项	说明
1	JX#**show policy-route** *NAME*	查看策略路由配置信息。

3.7.5 配置基于 ACL 的策略路由示例

组网需求

如下图所示，定义一条名为 aaa 的策略路由，所有从以太网接口 GE 1/0/1 接收的 IP 报文通过接口 GE 1/0/2 发送，下一跳 IP 是 192.168.1.2，其它报文仍然按照查找路由表的方式转发。

图 3-5 配置策略路由组网示意图



配置步骤

步骤 1 定义访问控制列表，ACL filter 1 匹配 IP 报文。

```
switch(config)#acl-ipv4 1001
```

```
switch(configure-acl-ipv4-1001)#rule 1 src-ip any dst-ip any
switch(configure-acl-ipv4-1001)#rule 1 action permit
```

步骤 2 定义策略的规则和动作。

```
switch(config)#policy-route aaa permit node 1
switch(config-policy-route-aaa-1)#if-match acl-ipv4 1001
switch(config-policy-route-aaa-1)#apply ip-address next-hop 192.168.1.2
switch(config-policy-route-aaa-1)#quit
```

步骤 3 在接口上使能策略。

```
switch(config)#inter ge 1/0/1
switch(config-ge-1/0/1)#policy-route bind-policy aaa
```

检查结果

```
switch(config-ge-1/0/1)#show policy-route aaa
policy-route : aaa
Node 1 : permit
if-match acl-ipv4 1001
apply ip-address next-hop 192.168.1.2
 enabled port : ge-1/0/1
```

4 DHCP

本章介绍 DHCP 的基本原理和配置过程，并提供相关的配置案例。

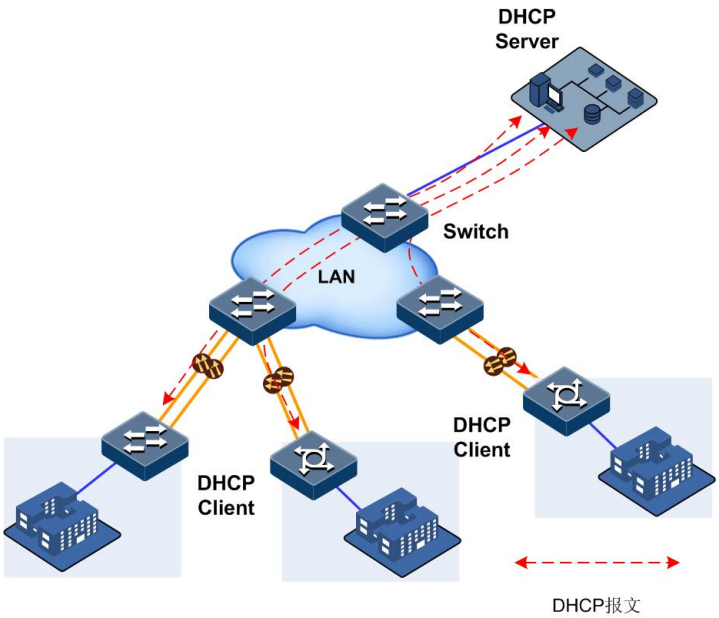
- 零配置
- DHCP Client
- DHCP Server
- DHCP Relay

4.1 零配置

4.1.1 简介

零配置功能是指设备无需进行任何手动配置，加电后，向零配置服务器自动发送申请 IP 地址的 DHCP 报文；当设备从零配置服务器获取 IP 后，自动下载服务器中的配置文件，自动更新自身配置。设备通过零配置服务器实现远端零配置的组网如图 4-1 所示。

图 4-1 零配置服务器组网示意图



注意

缺省情况下，设备零配置模式打开。当用户不需要使用零配置功能时，建议关闭零配置功能。

4.1.2 配置准备

场景

远端设备加电即可自动申请 IP 地址，无需手工配置。当用户需要更改零配置功能参数时，可根据本节内容进行配置。

前提

- 设备与 DHCP 服务器连接正确，且 DHCP 服务器已经正确配置。
- 连接零配置服务器的物理层接口状态为 UP。
- 上联交换机需要允许零配置远端设备中的某一 VLAN 通过。
- 设备配置为空。

4.1.3 零配置缺省配置

设备缺省配置如下。

功能	缺省值
零配置模式	零配置下缺省使能

4.1.4 配置零配置功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)# **ztp client start** { **startup-config** | **image** | **uboot** | **reboot-delaytime-after-upgraded** *delay-time* }* JX(config)# **ztp client stop**	配置 ZTP 功能。 缺省情况下，设备零配置启动时 ZTP 功能使能。 **注意** 当用户不需要使用零配置功能时，可通过 **ztp client stop** 命令去使能 ZTP 功能。

4.1.5 检查配置

设备获取到 IP 地址后，可通过以下命令检查结果。

步骤	检查项	说明
1	JX# **show dhcp client** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 DHCP 客户端配置信息和自动获取的信息。

4.2 DHCP Client

4.2.1 简介

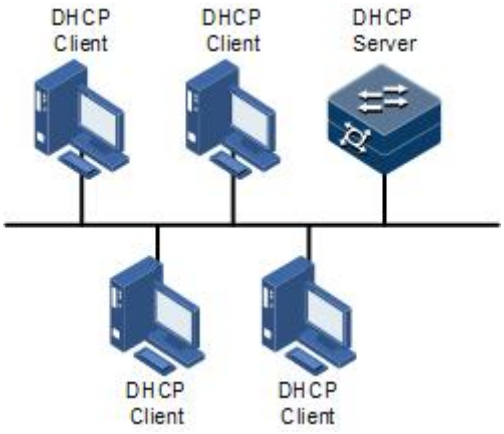
DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）在 TCP/IP 网络上给用户动态分配 IP 地址等配置信息的协议。它是基于 BOOTP（Bootstrap Protocol）协议，并在 BOOTP 协议的基础上添加了自动分配可用网络地址、网络地址重复使用以及其他扩展配置选项等功能。

随着网络规模的不断扩大和网络复杂度的提高，计算机的数量经常超过可供分配的 IP 地址数量。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。DHCP 就是为解决这些问题而发展起来的。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请（包括 IP 地址、子网掩码、缺省网关等参数），服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机），如图 4-2 所示。

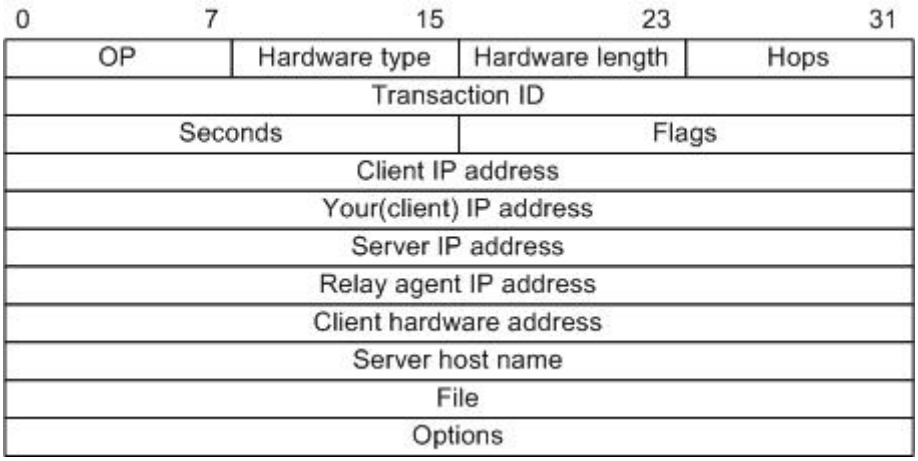
图 4-2 DHCP 典型应用组网示意图



DHCP 技术保证了 IP 地址的合理分配问题，从而避免了 IP 地址的浪费，提高了整网的 IP 地址使用率。

DHCP 报文格式如图 4-3 所示。DHCP 报文被封装在 UDP 数据报中。

图 4-3 DHCP 报文结构示意图



DHCP 报文中的各个字段含义如表 4-1 所示。

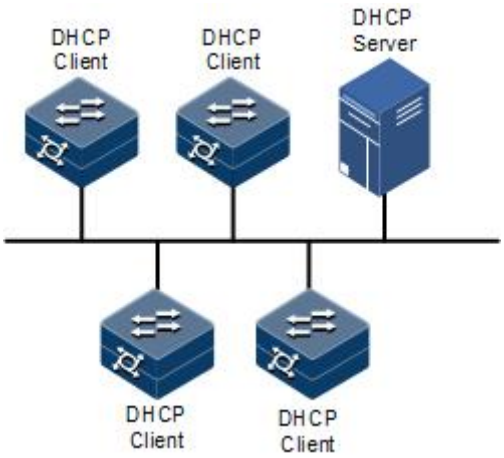
表 4-1 DHCP 报文字段含义列表

字段名	字段长度（Byte）	描述
OP	1	报文类型。 • 取值为 1 时，表示该报文为客户端请求报文； • 取值为 2 时，表示该报文为服务器端回应报文。
Hardware type	1	DHCP 客户端的硬件地址类型。
Hardware length	1	DHCP 客户端的硬件地址长度。
Hops	1	DHCP 报文经过的 DHCP 中继的数目。 DHCP 请求报文每经过一个 DHCP 中继，该字段就会加 1。
Transaction ID	4	客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。
Seconds	2	DHCP 客户端开始 DHCP 请求后所经过的时间。目前没有使用，固定为 0。
Flags	2	第 1 个比特为广播回应标识位，用来标识 DHCP 服务器回应报文是采用单播还是广播方式发送。 • 0 表示采用单播方式； • 1 表示采用广播方式。 其它比特保留不用。
Client IP address	4	DHCP 客户端的 IP 地址，只有当客户端在绑定，更新或重新绑定状态时进行填充，且可以用于回应 ARP 请求。
Your(client) IP address	4	DHCP 服务器分配给客户端的 IP 地址。
Server IP address	4	DHCP 服务器的 IP 地址。
Relay agent IP address	4	DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。
Client hardware address	16	DHCP 客户端的硬件地址。
Server host name	64	DHCP 服务器的名称。
File	128	DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。

字段名	字段长度（Byte）	描述
Options	可变	可选变长选项字段，包含报文的类型、有效租期、DNS（Domain Name System，域名系统）服务器的 IP 地址、WINS（Windows Internet Name Server ，Windows 网际命名服务）服务器的 IP 地址等配置信息。

设备支持作为 DHCP 客户端，从 DHCP 服务器获取 IP 地址，以便后续对该设备进行管理，如图 4-4 所示。

图 4-4 DHCP 客户端组网示意图



4.2.2 配置准备

场景

设备作为 DHCP 客户端时，从指定的 DHCP 服务器获取 IP 地址，可以用于后续对该设备的管理。

当采用动态地址分配方式时，DHCP 客户端所分配到的 IP 地址有一定的租借期限。租借期满后，DHCP 服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要续租 IP 地址。如果租借期未满，DHCP 客户端不需要继续使用该地址，可以释放 IP 地址。

若 DHCP 客户端需要通过多台 DHCP 中继向 DHCP 服务器获取 IP 地址，建议 DHCP 中继的台数不超过 4 台。

前提

在配置 DHCP 客户端之前，需完成以下任务：

- 创建 VLAN 并将接口加入 VLAN；
- 设备未启动 DHCP Snooping 功能。DHCP 客户端的缺省配置

设备上 DHCP 客户端的缺省配置如下。

功能	缺省值
hostname	设备主机名
class-id	缺省值可由启动参数指定
client-id	01 MAC

4.2.3 配置 DHCP 客户端

DHCP 客户端申请 IP 地址，需先创建 VLAN，同时配置好 DHCP 服务器，否则接口通过 DHCP 获取 IP 地址会失败。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入三层物理接口配置模式或者 VLAN 接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
4	JX (config-vlanif-*)#**dhcp client** { **class-id ascii** *class-id* | **client-id ascii** *client-id* | **hostname ascii** *host-name* }	配置 DHCP 客户端信息，可以配置的信息有类型标识符、客户端标识符和主机名称。 **注意** DHCP 客户端获取到 IP 地址后，不允许修改客户端信息。
4	JX (config-vlanif-*)#**ip address dhcp enable**	配置通过 DHCP 方式申请 IP 地址。
6	JX(config-vlan*)#**ip address dhcp renew**	续租 IP 地址。 若此前设备的 VLAN 接口通过 DHCP 方式获取了 IP 地址，在 IP 地址租约到期时将会自动续租。
7	JX(config-vlan*)#**ip address dhcp release**	释放 IP 地址。

4.2.4 配置 DHCPv6 客户端

DHCPv6 客户端申请 IPv6 地址，需先创建 VLAN，同时配置好 DHCPv6 服务器，否则接口通过 DHCP v6 获取 IPv6 地址会失败。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入三层物理接口配置模式或者 VLAN 接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
3	JX (config-vlanif-*)# **dhcpv6 client pd prefix-name** *prefix-name*	配置 DHCPv6 PD 客户端功能，将接口配置为 DHCPv6 PD 客户端的上联口，并配置接口上的前缀名。
4	JX(config-vlanif-*)#**dhcpv6 client pd renew**	续租 IPv6 前缀地址。
5	JX(config-vlanif-*)#**dhcpv6 client pd release**	释放 IPv6 前缀地址。
6	JX (config-vlanif-*)#**dhcpv6 client address prefix-name** *prefix-name* **prefix** *prefix/prefix-len*	将接口配置为 DHCPv6 PD 客户端的下联口，并配置接口上的前缀名和接口标识。前缀名必须和上联口配置的前缀名相同。

4.2.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

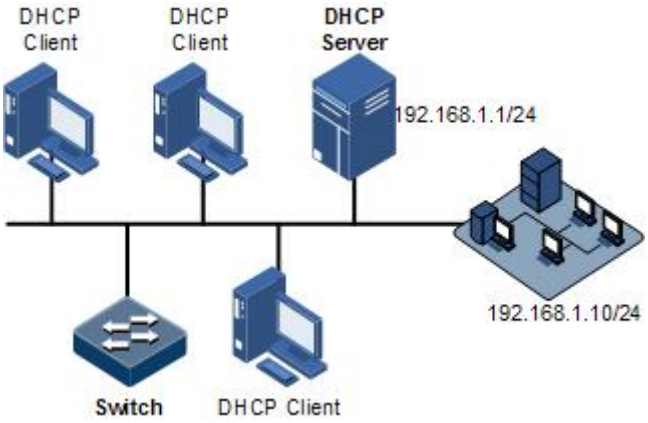
序号	检查项	说明
1	JX#**show dhcp client** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 DHCP 客户端配置信息。
2	JX#**show dhcpv6 config**	查看 DHCPv6 的配置信息。

4.2.6 配置 DHCP 客户端示例

组网需求

如图 4-5 所示，Switch 作为 DHCP 客户端，主机名为 JX，接入 DHCP 服务器和网管平台。需要由 DHCP 服务器分配 IP 地址给 Switch，从而使网管平台能够管理 Switch。

图 4-5 配置 DHCP 客户端组网示意图



配置步骤

步骤 1 配置 DHCP 客户端信息。

```
JX#configure
JX(config)#interface vlan 1
JX(config-vlanif-1)#dhcp client hostname ascii JX
```

步骤 2 配置通过 DHCP 方式申请 IP 地址。

```
JX(config-vlanif-1)#ip address dhcp enable
```

检查结果

通过 **show dhcp client** 命令查看 DHCP 客户端配置是否正确。

```
JX#show dhcp client
Interface vlan-1 dhcp client information :
-------------------------------------------------------------
  Current state : Bound
  Allocated IP : 192.168.1.2
  Subnet Mask : 255.255.255.0
  Server IP : 192.168.1.1
  Allocated lease : 86400 seconds
  Lease T1 time : 43200 seconds
  Lease T2 time : 75600 seconds
  Lease Obtained : 2023/07/18  Tue  18:49:37
  Lease  timeout : 2023/07/19  Wed  18:49:37
  Transaction ID : 0x5558ec
  Client ID :
  Class ID :
  Hostname : JX
  DNS :
  Getway :
  Domain :
  Lease : 0 days 23 hours 59 minutes 49 seconds.
```

4.3 DHCP Server

4.3.1 简介

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是在 TCP/IP 网络上给用户动态分配 IP 地址等配置信息的协议。它是基于 BOOTP（Bootstrap Protocol）协议，并在 BOOTP 协议的基础上添加了自动分配可用网络地址、网络地址重复使用以及其他扩展配置选项等功能。

随着网络规模的不断扩大和网络复杂度的提高，计算机的数量经常超过可供分配的 IP 地址数量。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。DHCP 就是为解决这些问题而发展起来的。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请（包括 IP 地址、子网掩码、缺省网关等参数）服务器端返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

在 DHCP 的客户端/服务器通信模式中指定专门的主机分配网络地址，传送网络配置参数给需要的网络主机，被指定的主机称为 DHCP Server。

DHCP 应用

一般情况下，在以下场合会利用 DHCP Server 来完成 IP 地址分配：

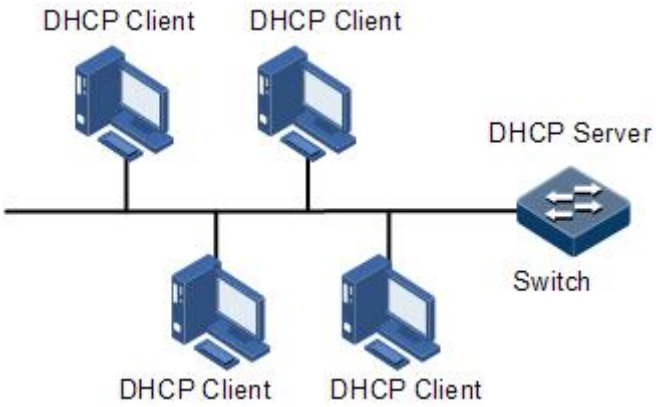
- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址，且对同时接入网络的用户数目也有限制。
- 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定 IP 地址需求。

DHCP Client 从 DHCP Server 获得 IP 地址后，并不能永久使用其获得的 IP 地址，而是有一个固定的使用期限，称为租约时间。

DHCP 技术解决了 IP 地址的合理分配问题，从而避免了 IP 地址的浪费，提高了整网的 IP 地址使用率。

设备支持作为 DHCP Server，向客户端提供动态 IP 地址，如图 4-6 所示。

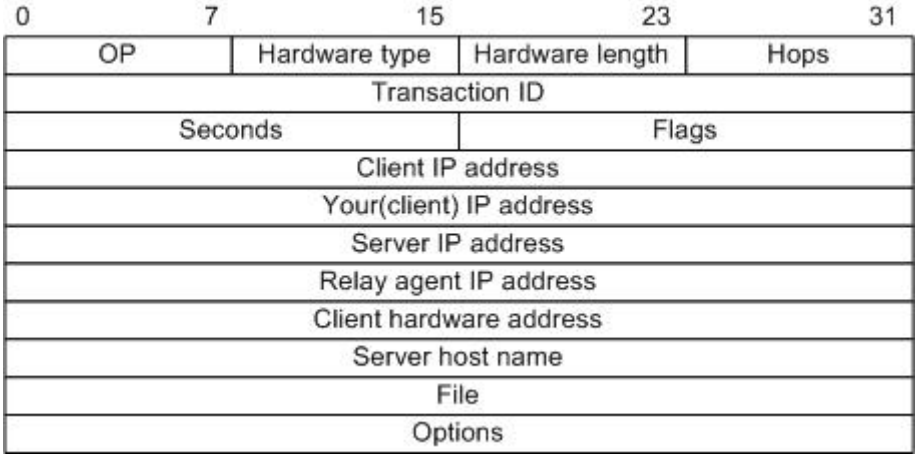
图 4-6 DHCP Server 和 DHCP Client 应用组网示意图



DHCP 报文

DHCP 报文格式如图 4-7 所示。DHCP 报文被封装在 UDP 数据报中。

图 4-7 DHCP 报文结构示意图



DHCP 报文中的各个字段含义如表 4-2 所示。

表 4-2 DHCP 报文字段含义列表

字段名	字段长度（Byte）	描述
OP	1	报文类型。 • 取值为 1 时，表示该报文为客户端请求报文； • 取值为 2 时，表示该报文为服务器端回应报文。
Hardware type	1	DHCP 客户端的硬件地址类型。

字段名	字段长度（Byte）	描述
Hardware length	1	DHCP 客户端的硬件地址长度。
Hops	1	DHCP 报文经过的 DHCP 中继的数目。 DHCP 请求报文每经过一个 DHCP 中继，该字段就会加 1。
Transaction ID	4	客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。
Seconds	2	DHCP 客户端开始 DHCP 请求后所经过的时间。目前没有使用，固定为 0。
Flags	2	第 1 个比特为广播回应标识位，用来标识 DHCP 服务器回应报文是采用单播还是广播方式发送。 • 0 表示采用单播方式； • 1 表示采用广播方式。 其它比特保留不用。
Client IP address	4	DHCP 客户端的 IP 地址，只有当客户端在绑定，更新或重新绑定状态时进行填充，且可以用于回应 ARP 请求。
Your(client) IP address	4	DHCP 服务器分配给客户端的 IP 地址。
Server IP address	4	DHCP 服务器的 IP 地址。
Relay agent IP address	4	DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。
Client hardware address	16	DHCP 客户端的硬件地址。
Server host name	64	DHCP 服务器的名称。
File	128	DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。
Options	可变	可选变长选项字段，包含报文的类型、有效租期、DNS（Domain Name System，域名系统）服务器的 IP 地址、WINS（Windows Internet Name Server ，Windows 网际命名服务）服务器的 IP 地址等配置信息。

DHCPv6

DHCPv6 是一种运行在客户端和服务器之间的协议，与 IPv4 中的 DHCP 一样，所有的协议报文都是基于 UDP 的。但是由于在 IPv6 中没有广播报文，因此 DHCPv6 使用组播报文，客户端也无需配置服务器的 IPv6 地址。

4.3.2 配置准备

场景

设备作为 DHCPv4 服务器时，DHCPv4 客户端可以向设备获取 IP 地址。

前提

接口上必须配置 IP 地址，且该接口未启动 DHCP 客户端和 DHCP Relay。

4.3.3 创建并配置 IPv4 地址池

请在需要创建并配置 IPv4 地址池的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**dhcp start**	使能全局 DHCP 功能。
3	JX(config)#**dhcp server pool** *pool-name*	创建 IPv4 地址池并进入地址池配置模式。
4	JX(config-dhcp-pool-*)#**ip range** *start-ip-address end-ip-address* **mask** *mask*	配置 IPv4 地址池的地址范围。
5	JX(config-dhcp-pool-*)#**dhcp server exclude-ip** *start-ip-address* [*end-ip-address*]	配置 IPv4 地址池排除的地址范围。
6	JX(config-dhcp-pool-*)#**lease-time** { *hour* | **day** *day* **hour** *hour* **minute** *minute* | **unlimited** | **default** }	配置 IPv4 地址池的地址租期。
7	JX(config-dhcp-pool-*)#**dns** *ip-address* [**backup**]	配置 IPv4 地址池的 DNS 服务器。
8	JX(config-dhcp-pool-*)#**gateway** *ip-address*	配置 IPv4 地址池的缺省网关。
9	JX(config-dhcp-pool-*)#**option** *option-code* [**sub-option** *option-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** ip-address }	配置 Option 携带信息。
10	JX(config)#**dhcp server static-bind** *ip-address mac-address*	配置 IPv4 地址池中的 IP 地址与用户 MAC 地址绑定。

4.3.4 配置接口的 DHCP Server 功能

请在需要配置接口的 DHCP 服务器功能的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式或者三层物理接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
3	JX(config-vlanif-*)#**dhcp enable server**	使能接口的 DHCPv4 服务器功能。

4.3.5 回收 IP 地址或地址池

请在需要回收 IP 地址池的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**no dhcp server pool** *pool-name*	回收 IP 地址池。
3	JX(config)#**no dhcp server user-bind**	回收 DHCPv4 服务器的地址绑定表。
4	JX(config)#**no dhcp server dynamic-bind** *ip-address*	回收与用户 MAC 地址绑定的 IP 地址。

4.3.6 配置 DHCPv4 Server Ping 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**dhcp server address-check-time** { *period* | **default** }	配置 DHCP Server 分配地址前检查地址是否被使用所等待的超时时间。0 表示不检查地址是否被使用，默认 500ms

4.3.7 创建并配置 IPv6 地址池

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dhcpv6 start**	使能全局 DHCPv6 功能。
3	JX(config)#**dhcpv6 server pool** *pool-name*	创建 IPv6 地址池并进入地址池配置模式。
4	JX(config-dhcpv6-pool-*)#**address-delegation prefix** *prefix/prefix-len*	配置 IPv6 地址池的前缀和前缀长度。
5	JX(config-dhcpv6-pool-*)#**dns-server** *ipv6-address*	配置 IPv6 地址池的 DNS 服务器。
6	JX(config-dhcpv6-pool-*)#**domain-name** *domain-name*	配置 IPv6 地址池的域名服务器。
7	JX(config-dhcpv6-pool-*)#**sntp-server** *ipv6-address*	配置 IPv6 地址池的 SNTP 服务器。

4.3.8 配置接口的 DHCPv6 服务器功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式或者三层物理接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
3	JX(config-vlanif-*)#**dhcpv6 enable server**	使能接口的 DHCPv6 服务器功能。
4	JX(config-vlanif-*)#**dhcpv6 server bind-pool** *pool-name*	配置 DHCPv6 server 接口上引用的地址池。

4.3.9 回收 IPv6 地址池

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**no dhcpv6 server pool** *pool-name*	回收 IPv6 地址池。

4.3.10 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show dhcp server config	查看 DHCP 服务器的配置信息。
2	JX#show dhcp information	查看 DHCP 服务器的详细信息。
3	JX#show dhcp server user-bind	查看已分配的 IP 地址及其客户端信息。
4	JX#show dhcp server statistics	查看 DHCP 服务器的报文统计信息。
5	JX#show dhcp server pool	查看 DHCP 服务器的地址池配置信息。
6	JX#show dhcpv6 config	查看 DHCPv6 的配置信息。
7	JX#show dhcpv6 statistics	查看 DHCPv6 的报文统计信息。
8	JX#show dhcpv6 server user-bind	查看已分配的 IPv6 地址及其客户端信息。
9	JX#show dhcpv6 server pool	查看 DHCPv6 服务器的地址池配置信息。

4.3.11 维护

用户可以通过以下命令，维护设备 DHCP Server 特性的运行情况和配置情况。

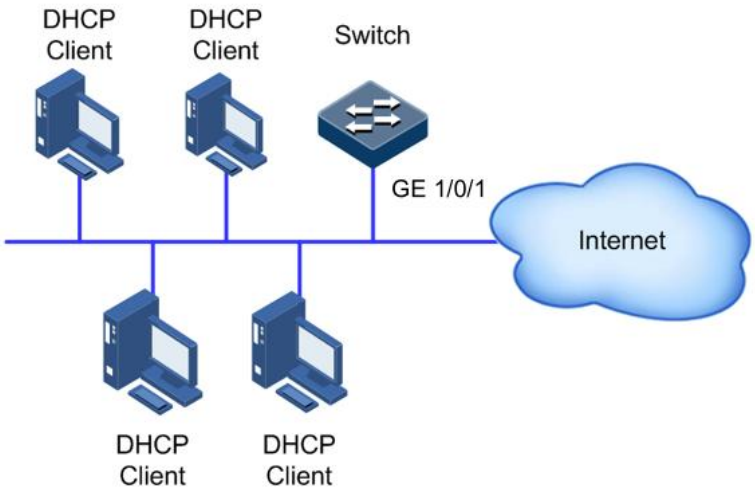
命令	描述
JX(config)# reset dhcp server statistics	清空 DHCP Server 统计信息。
JX(config)#reset dhcpv6 statistics	清空 DHCPv6 统计信息。

4.3.12 配置 DHCPv4 服务器示例

组网需求

如图 4-8 所示，Switch 设备作为 DHCP 服务器分配 IP 地址给 DHCP 客户端，租期为 8 小时，IP 地址池名称为 pool，IP 地址范围是 172.31.1.2～172.31.1.100，DNS 服务器的 IP 地址为 172.31.100.1。

图 4-8 配置 DHCP 服务器组网示意图



配置步骤

步骤 1 创建并配置 IP 地址池。

```
JX#configure
JX(config)#dhcp start
JX(config-dhcp-pool-1)#dhcp server pool 1
JX(config-dhcp-pool-1)# ip range 172.31.1.2 172.31.1.100 mask
255.255.255.0
JX(config-dhcp-pool-1)#lease-time day 0 hour 8 minute 0
JX(config-dhcp-pool-1)#dns 172.31.100.1
JX(config-dhcp-pool-1)#exit
```

步骤 2 配置接口的 DHCP 服务器功能。

```
JX(config)#interface vlan 1
JX(config-vlanif-1)#ip address 172.31.1.1/24
JX(config-vlanif-1)#dhcp enable server
```

检查结果

通过 **show dhcp server config** 命令查看 DHCP 服务器配置是否正确。

```
JX# show dhcp server config
!
dhcp start
dhcp server pool 1
ip range 172.31.1.2 172.31.1.100 mask 255.255.255.0
dns 172.31.100.1
lease-time day 0 hour 8 minute 0
!
interface vlan 1
dhcp enable server
```

通过 **show dhcp server pool** 命令查看 DHCP 服务器的地址池配置是否正确。

```
JX# show dhcp server pool

DHCP Pool 1 information :
-------------------------------------------------------------
 IP range               : 172.31.1.2 to 172.31.1.100
 Mask                   : 255.255.255.0
 Gateway                : 0.0.0.0
 DNS                    : main : 172.31.100.1 , backup : 0.0.0.0
 Lease                  : 0 days 8 hours 0 minutes
 Total Number           : 99
 Used Number            : 0
-------------------------------------------------------------
```

4.4 DHCP Relay

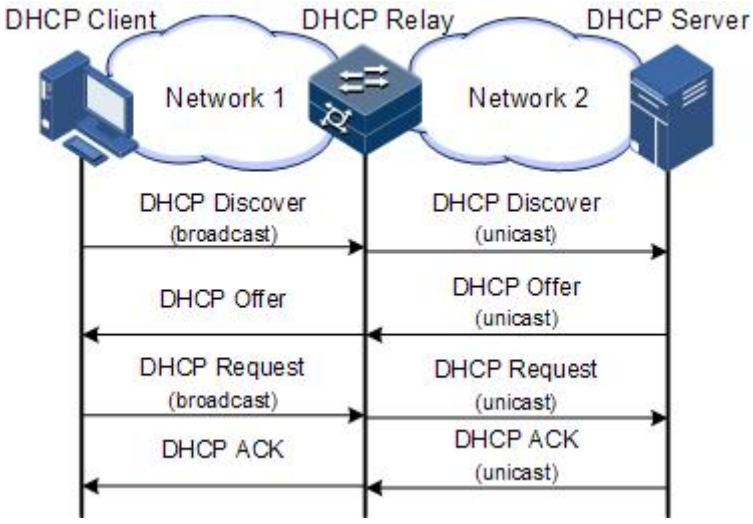
4.4.1 简介

最初的 DHCP 协议要求客户端和 DHCP 服务器只能在一个网段内，不可以跨网段工作。因此，为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是不经济的。

DHCP Relay（DHCP 中继）的引入解决了这个问题，它可使处于不同网段间的 DHCP 客户端和 DHCP 服务器之间承担中继服务，将 DHCP 协议报文跨网段中继到目的 DHCP 服务器，于是处在不同网段的 DHCP 客户端可以共同使用同一个 DHCP 服务器。

DHCP Relay 工作原理如图 4-9 所示。

图 4-9 DHCP Relay 工作原理示意图



DHCP 客户端发送请求报文给 DHCP 服务器，DHCP 中继在收到该报文并适当处理后，发送给指定网段上的 DHCP 服务器。服务器根据请求报文中提供的必要信息，通过 DHCP 中继返回给客户端，完成对客户端的动态配置。

4.4.2 配置准备

场景

当 DHCP 客户端和 DHCP 服务器不在同一网段时，可以使用 DHCP Relay 功能解决这一问题。它可使处于不同网段间的 DHCP 客户端和 DHCP 服务器之间承担中继服务，将 DHCP 协议报文跨网段中继到目的 DHCP 服务器，于是处在不同网段的 DHCP 客户端可以共同使用同一个 DHCP 服务器。

前提

无

4.4.3 DHCP Relay 的缺省配置

设备上 DHCP Relay 的缺省配置如下。

功能	缺省值
全局 DHCP Relay 功能状态	禁止
接口 DHCP Relay 功能状态	禁止
全局 DHCPv6 Relay 功能状态	禁止
接口 DHCPv6 Relay 功能状态	禁止

4.4.4 配置接口的 DHCP Relay 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**dhcp start**	使能全局 DHCP 功能。
3	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式或者三层物理接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
3	JX(config-vlanif-*)#**dhcp enable relay**	使能接口下 DHCP Relay 功能。
4	JX(config-vlanif-*)#**dhcp relay server-ip** *ip-address*	配置 DHCP 服务器的 IP 地址。

4.4.5 配置接口的 DHCPv6 Relay 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**dhcpv6 start**	使能全局 DHCPv6 功能。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式或者三层物理接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
3	JX(config-vlanif-*)#**dhcpv6 enable relay**	使能接口下 DHCPv6 Relay 功能。
4	JX(config-vlanif-*)#**dhcpv6 relay destination** *ipv6-address*	配置 DHCPv6 服务器的 IPv6 地址。

4.4.6 配置 DHCP Relay 支持 Option 82 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式或者三层物理接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
3	JX(config-vlanif-*)#**dhcp relay option82 enable**	配置 DHCP Relay 支持 Option 82。
4	JX(config-vlanif-*)#**dhcp relay option82** { **drop** | **keep** | **replace** }	配置 DHCP Relay 对含 Option 82 的 DHCP 请求报文处理策略。
5	JX(config-vlanif-*)#**dhcp relay option82 circuit-id format** { **default** | **user-defined** format-string }	配置 DHCP Relay Option82 的 circuitID 字段内容
6	JX(config-vlanif-*)#**dhcp relay option82 remote-id format** { **default** | **user-defined** format-string }	配置 DHCP Relay Option82 的 remoteID 字段内容

4.4.7 配置 DHCPv6 Relay 支持 Option 18/37 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**dhcpv6 relay interface-id format** { **default** | **user-defined** format-string }	配置 DHCPv6 报文中的 interface-id 选项（option 18）的格式。
3	JX(config)#**dhcpv6 relay remote-id format** { **default** | **user-defined** format-string }	配置 DHCPv6 报文中的 remote-id 选项（option 37）的格式。
4	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式或者三层物理接口配置模式，以下以 VLAN 接口配置模式为例进行说明。
5	JX(config-vlanif-*)#**dhcpv6 relay interface-id enable**	配置 DHCPv6 Relay 支持 Option 18。
3	JX(config-vlanif-*)#**dhcpv6 relay remote-id enable**	配置 DHCPv6 Relay 支持 Option 37。

4.4.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show dhcp relay config**	查看 DHCP Relay 功能配置信息。
2	JX#**show dhcp relay user-bind**	查看 DHCP Relay 的绑定信息。
3	JX#**show dhcp relay statistics**	查看 DHCP Relay 的报文统计信息。
4	JX#**show dhcpv6 config**	查看 DHCPv6 Relay 的配置信息。
5	JX#**show dhcpv6 statistics**	查看 DHCPv6 Relay 的报文统计信息。

4.4.9 维护

用户可以通过以下命令，维护设备 DHCP RELAY 特性的运行情况和配置情况。

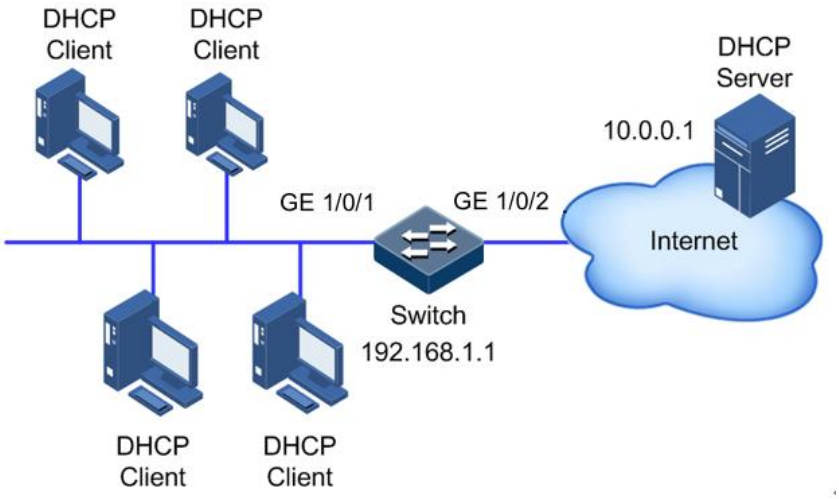
命令	描述
JX(config)#**reset dhcp relay statistics**	清空 DHCP Relay 统计信息。
JX(config)#**reset dhcpv6 statistics**	清空 DHCPv6 统计信息。

4.4.10 配置 DHCPv4 中继示例

组网需求

如图 4-10 所示，Switch 设备作为 DHCP 中继，主机名为 JX，通过业务接口接入 DHCP 服务器。需要由 DHCP 服务器分配 IP 地址给客户端设备，从而使网管平台能够发现并管理该设备。

图 4-10 配置 DHCP 中继组网示意图



配置步骤

步骤 1 配置接口的 DHCP Relay 功能。

```
JX#config
JX(config)#dhcp start
JX(config)#interface vlan 1
JX(config-vlanif-1)#ip address 192.168.1.1/24
JX(config-vlanif-1)#dhcp enable relay
JX(config-vlanif-1)#dhcp relay server-ip 10.0.0.1
JX(config-vlanif-1)#exit
```

检查结果

通过 **show dhcp relay config** 命令查看 DHCP 中继配置是否正确。

```
JX#show dhcp relay config
!
dhcp start
!
interface vlan 1
dhcp enable relay
dhcp relay server-ip 10.0.0.1
```

5 QoS

本章介绍 QoS 的基本原理和配置过程，并提供相关的配置案例。

- 简介
- 优先级映射
- 队列调度
- 拥塞避免
- 流量限速

5.1 简介

随着网络应用种类的日益丰富，用户对不同的网络应用提出了不同的服务质量需求，这就需要网络能够根据用户的需求为不同的网络应用分配和调度资源。QoS（Quality of Service，服务质量）技术的产生，使网络在发生过载或拥塞时，能够确保重要业务的实时性和完整性，同时保证整个网络的高效运行。

QoS 由一组流量管理技术组成：

- 服务模型
- 优先级信任
- 流分类
- 流策略
- 优先级映射
- 拥塞管理
- 拥塞避免

5.1.1 服务模型

QoS 技术服务模型：

- Best-effort Service（尽力而为服务模型）
- Differentiated Service（区分服务模型，简称 DiffServ）

Best-effort

Best-effort 服务模型是基于储存转发机制的 Internet（IPv4 标准）最基本、最简单的服务模型。在 Best-effort 服务模型中，应用程序在任何时刻，发送任意数量的报文，而且事先不需要经过批准，也不需要通知网络。对 Best-effort 服务来说，网络尽最大可能来发送报文，但对时延、可靠性等不做任何保证。

Best-effort 模型是现在 Internet 缺省的服务模型，适用于大多数网络应用，如 FTP，E-mail 等，它通过先入先出（FIFO）队列来实现。

DiffServ

DiffServ 模型是一个多服务模型，它可以满足不同的 QoS 需求。

对于 DiffServ 模型来说，它不需要为每个流维护状态。它根据每个报文的 QoS 分类来提供差异化的服务。可以使用不同的方法进行报文的 QoS 分类，如 IP 报文的优先级（IP Precedence）、报文的源地址或目的地址等。

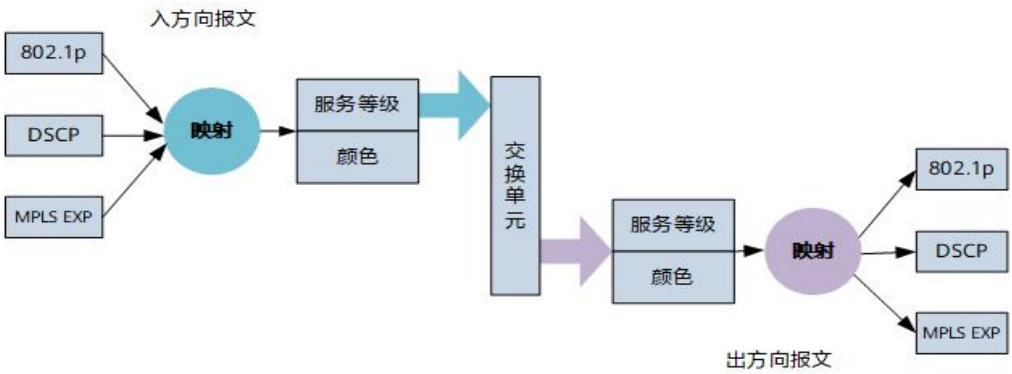
DiffServ 一般用来为一些重要的应用提供端到端的 QoS 服务。主要通过以下技术来实现：

- CAR（Committed Access Rate，承诺访问速率）：根据预先设定的报文匹配规则。如 IP 报文的优先级、报文的源地址或目的地址等，进行报文的分类。如果是符合令牌桶流量规则的报文，就继续发送。如果是超出流量规定的报文，则被丢弃或者重新标记 IP Precedence、DSCP、EXP 等。CAR 不仅可以进行流量控制，还可以对报文进行标记和重标记。
- 队列技术：SP、WRR、WFQ、SP+WRR、SP+WFQ 等队列技术对拥塞的报文进行缓存和调度，实现拥塞管理。

5.2 优先级映射

5.2.1 简介

优先级映射



服务等级是指报文在设备内部的服务质量，它决定了报文在设备内部所属的队列类型。服务等级有 8 种取值，即 8 种 PHB（Per-Hop Behavior），优先级从高到低依次为 CS7、CS6、EF、AF4、AF3、AF2、AF1、BE。PHB 行为的详细描述，参见 PHB 行为。

颜色是指报文在设备内部的丢弃优先级，用于决定同一个队列内部当队列发生拥塞时报文的丢弃顺序。颜色有 3 种取值，IEEE 定义的优先级从低到高依次为 Green、Yellow、Red。丢弃优先级的高低实际取决于对应参数的配置。

在每一个 DS 节点上对报文的处理称为 PHB。PHB 描述了 DS 节点对报文采用的外部可见的转发行为。PHB 可以用优先级来定义，也可以用一些可见的服务特征如报文延迟、抖动或丢包率来定义。PHB 只定义了一些外部可见的转发行为，没有指定特定的实现方式。

RFC 定义了四种标准的 PHB：CS（Class Selector），EF（Expedited Forwarding），AF（Assured Forwarding）和 BE（Best-Effort）。其中，BE 是缺省的 PHB。

在 RFC 2474 中，CS 又被划分为两个等级，即 CS6 和 CS7；在 RFC 2597 中，AF 又被划分为四个等级，即为 AF1～AF4。至此，PHB 共有 8 个细分级别，每个 PHB 在设备内部都有对应的服务等级，不同的服务等级将决定不同流的拥塞管理策略。同时每个 PHB 又再被划分为三个颜色（Color，也可以叫丢弃优先级），分别用 Green、Yellow 和 Red 表示，不同的颜色将决定不同流的拥塞避免策略。

优先级信任

优先级信任是指设备采用报文自身携带的优先级作为分类依据，对报文进行后续的 QoS 管理操作。

信任的优先级种类有：

- 基于 DSCP（Differentiated Services Code Point，差分服务代码点）优先级
- 基于 8021p inner 优先级
- 基于 8021p outer 优先级

5.2.2 配置准备

场景

对于来自上游设备的报文，用户可以选择信任报文携带的优先级，对于不信任其优先级的报文可以交由流分类和流策略处理。配置优先级信任模式后，设备可以依据不同优先级对报文进行相应的操作，提供相应的服务。

为报文指定本地优先级是进行队列调度的前提条件，对于来自上游设备的报文，用户可以将报文携带的外部优先级映射到不同的本地优先级，也可以基于接口直接配置报文的本地优先级，之后设备将依据本地优先级对报文进行队列调度。通常来说，对于 IP 报文，需要配置 IP 优先级或 DSCP 优先级与本地优先级的映射关系；对于 VLAN 报文，需要配置 8021p outer 优先级与本地优先级的映射关系。

前提

无

5.2.3 基本 QoS 的缺省配置

设备上基本 QoS 的缺省配置如下。

功能	缺省值
全局 QoS 功能状态	使能
入接口信任的优先级类型	信任 8021p outer 优先级
出接口优先级重标记	去使能

表 5-1 缺省情况下 8021p 入方向和本地优先级及颜色的映射关系

802.1p 优先级	PHB 行为	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

表 5-2 缺省情况下 8021p 出方向和本地优先级及颜色的映射关系

PHB 行为	Color	802.1p 优先级
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3

PHB 行为	Color	802.1p 优先级
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

表 5-3 缺省情况下 DSCP 入方向和本地优先级及颜色的映射关系

DSCP	PHB 行为	Color
DSCP	PHB 行为	Color
0	BE	green
32	AF4	green
1	BE	green
33	BE	green
2	BE	green
34	AF4	green
3	BE	green
35	BE	green
4	BE	green
36	AF4	yellow
5	BE	green
37	BE	green

DSCP	PHB 行为	Color
6	BE	green
38	AF4	red
7	BE	green
39	BE	green
8	AF1	green
40	EF	green
9	BE	green
41	BE	green
10	AF1	green
42	BE	green
11	BE	green
43	BE	green
12	AF1	yellow
44	BE	green
13	BE	green
45	BE	green
14	AF1	red
46	EF	green
15	BE	green
47	BE	green
16	AF2	green
48	CS6	green
17	BE	green
49	BE	green
18	AF2	green
50	BE	green
19	BE	green
51	BE	green
20	AF2	yellow
52	BE	green
21	BE	green

DSCP	PHB 行为	Color
53	BE	green
22	AF2	red
54	BE	green
23	BE	green
55	BE	green
24	AF3	green
56	CS7	green
25	BE	green
57	BE	green
26	AF3	green
58	BE	green
27	BE	green
59	BE	green
28	AF3	yellow
60	BE	green
29	BE	green
61	BE	green
30	AF3	red
62	BE	green
31	BE	green
63	BE	green

表 5-4 缺省情况下 DSCP 出方向和本地优先级及颜色的映射关系

PHB 行为	Color	DSCP
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14

PHB 行为	Color	DSCP
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

5.2.4 配置入接口信任的优先级类型

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组接口配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/1)#**trust** { **8021p** | **diffserv** | **dscp** | **mpls-exp** | **none** }	在接口上设置信任的报文优先级

5.2.5 配置 DIFFSERV 模版

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**diffserv domain default**	创建 diffserv 域模版或者进入 default 模版 default：默认模版
3	JX(config-dsdomain-ds1)#**8021p-inbound** *8021p-value* **phb** { { **BE** | **AF1** | **AF2** | **AF3** | **AF4** | **EF** | **CS6** | **CS7** } [**green** | **yellow** | **red**] | **default** } JX(config-dsdomain-ds1)#**8021p-inbound default**	8021p-value： 8021p 优先级 BE|AF1|AF2|AF3|AF4|EF|CS6|CS7：8 个队列 green|yellow|red：3 种颜色
4	JX(config-dsdomain-ds1)#**8021p-outbound** { **BE** | **AF1** | **AF2** | **AF3** | **AF4** | **EF** | **CS6** | **CS7** } **map** { *8021p-value* | **default** }	8021p-value： 8021p 优先级 BE|AF1|AF2|AF3|AF4|EF|CS6|CS7：8 个队列 green|yellow|red：3 种颜色
5	JX(config-dsdomain-ds1)#**ip-dscp-inbound dscp-value phb** { **BE** | **AF1** | **AF2** | **AF3** | **AF4** | **EF** | **CS6** | **CS7** } [**green** | **yellow** | **red**]	dscp-value ： dscp 优先级 BE|AF1|AF2|AF3|AF4|EF|CS6|CS7：8 个队列 green|yellow|red：3 种颜色
6	JX(config-dsdomain-ds1)#**ip-dscp-outbound** { **BE** | **AF1** | **AF2** | **AF3** | **AF4** | **EF** | **CS6** | **CS7** } [**green** | **yellow** | **red**] **map dscp-value**	dscp-value ： dscp 优先级 BE|AF1|AF2|AF3|AF4|EF|CS6|CS7：8 个队列 green|yellow|red：3 种颜色

5.2.6 配置出接口 8021P/DSCP 重标记

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。

步骤	配置	说明
3	JX(config-ge-1/0/1)#**qos phb marking { 8021p | dscp } { enable | disable }**	使能/去使能再出接口上的内部优先级到外部优先级的重标记 8021p：重标记 8021p 优先级 Dscp：重标记 dscp 优先级

5.2.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show differv domain [config | name default]**	显示配置的 diffserv 域模版信息
2	JX#**show differv domain interface** *interface-type interface-number*	显示配置的 diffserv 域模板接口信息

5.3 队列调度

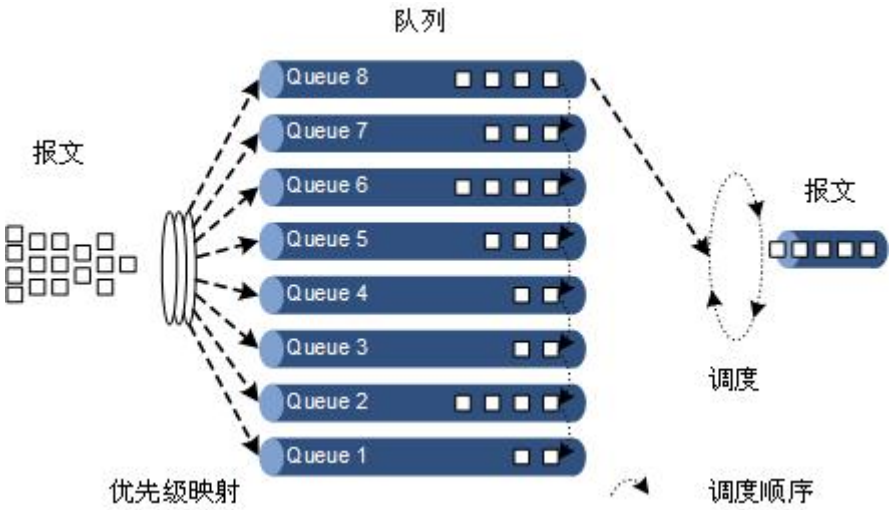
5.3.1 简介

当时延敏感业务要求得到比非时延敏感业务更高质量的 QoS 服务，或网络间歇性的出现拥塞时，需要进行队列调度。

队列调度是指使用不同的调度算法来发送队列中的报文流。设备支持的队列调度算法有 SP（Strict-Priority，严格优先级调度）、WRR（Weight Round Robin，加权循环调度）、WFQ（Weighted Fair Queueing，加权公平队列）、SP+WRR、SP+WFQ。每种调度算法都是为了解决特定网络流量的问题，并对带宽资源的分配、延迟、抖动等有不同的影响。

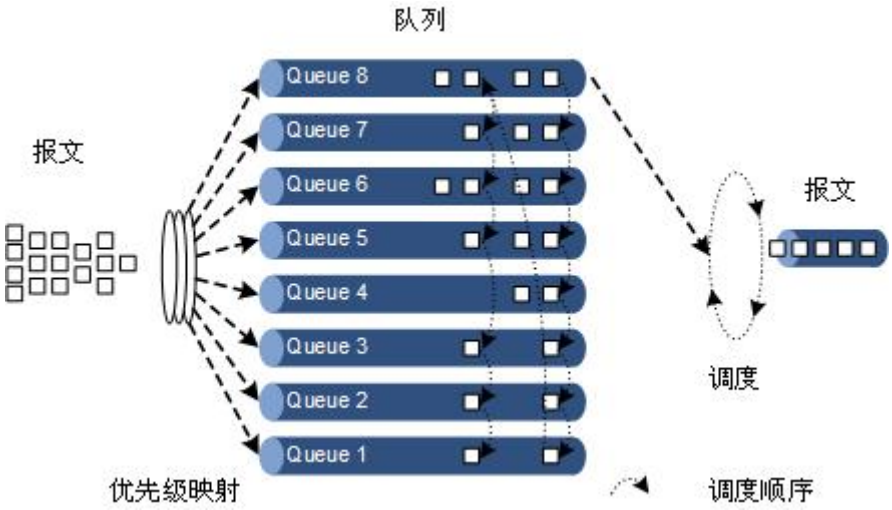
- SP：设备严格按照队列优先级的高低顺序进行调度。只有高优先级队列中的报文全部调度完毕后，低优先级队列才有调度的机会。如下图所示。

图 5-2 SP 调度示意图



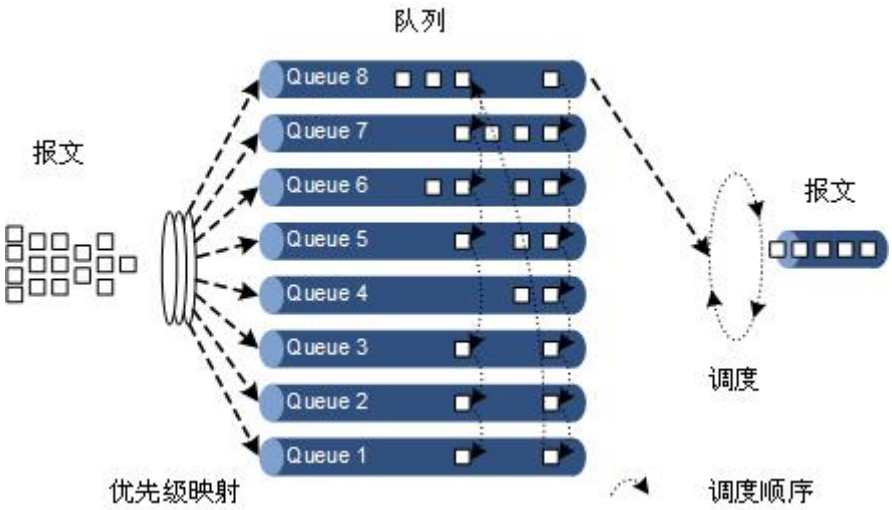
- WRR：在按照队列的优先级次序以循环方式调度每个队列报文的基础上，根据每个队列的权重，以报文个数来调度各队列中的报文。如下图所示。

图 5-3 WRR 调度示意图



- WFQ：在按照队列的优先级次序以循环方式调度每个队列报文的基础上，根据每个队列的权重，以 bit 为单位来调度各队列中的报文。如下图所示。

图 5-4 WFQ 调度示意图



- SP+WRR：SP 调度和 WRR 调度相结合的调度方式，将设备接口上的队列分为两组，用户可以指定其中的某几组队列进行 SP 调度，其他队列进行 WRR 调度。
- SP+WFQ：SP 调度和 WFQ 调度相结合的调度方式，将设备接口上的队列分为两组，用户可以指定其中的某几组队列进行 SP 调度，其他队列进行 WFQ 调度。

5.3.2 配置准备

场景

当网络发生拥塞时，若用户希望能均衡各类报文的延迟和延迟抖动，关键业务（如视频业务、语音业务）的报文能够得到优先处理；同时对于非关键业务（如 E-Mail）的报文，保证相同优先级业务得到公平处理，不同优先级业务按照各自权值处理。可以通过配置队列调度来实现。具体选择何种调度算法，需要依据当时的业务情况与客户需求。

前提

全局 QoS 功能使能。

5.3.3 队列调度的缺省配置

设备上队列调度的缺省配置如下。

功能	缺省值
队列调度模式	SP
队列权重	• WRR 调度 8 个队列的权重均为 1 • WFQ 调度 8 个队列的权重均为 1

5.3.4 配置 SP 队列调度

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组接口配置模式。以下步骤以二层物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**queue scheduling sp**	配置接口队列调度方式为 SP。

5.3.5 配置 WRR 或 SP+WRR 队列调度

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组接口配置模式。以下步骤以二层物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**queue scheduling wrr**	配置接口队列调度方式为 WRR。
4	JX(config-ge-1/0/*)#**queue** *queue-id* **weight** *weight-value*	配置各队列的权重。

5.3.6 配置 WFQ 或 SP+WFQ 队列调度

请在需要配置 WFQ 或 SP+WFQ 队列调度的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组接口配置模式。以下步骤以二层物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**queue scheduling wfq**	配置接口队列调度方式为 WFQ。
4	JX(config-ge-1/0/*)#**queue** *queue-id* **weight** *weight-value*	配置各队列的权重。

5.3.7 配置队列带宽保证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式或聚合组接口配置模式。以下步骤以二层物理接口配置模式为例。
3	JX(config-ge-1/0/1)# **queue** *queue-id* **{ min-bandwidth | max-bandwidth }** { **kbps | mbps | gbps** } *bandwidth* JX(config-ge-1/0/1)# **queue** *queue-id* **priority** { *priority* | **default** } JX(config-ge-1/0/1)# **queue** *queue-id* **weight** { *weight* | **default** }	配置基于接口队列的带宽保证。

5.3.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show queue interface { 10ge | ge }** *interface-number*	查看接口的队列信息。
2	JX#**show queue statistics interface { 10ge | ge }** *interface-number* JX#**show queue statistics interface all**	查看接口下队列的统计信息。

5.3.9 维护

用户可以通过以下命令，维护队列调度。

命令	描述
JX(config)#**reset queue statistics interface { 10ge | ge }** *interface-number* JX#(config)#**reset queue statistics interface all**	清空接口下队列对包数统计。

5.3.10 配置队列调度示例

组网需求

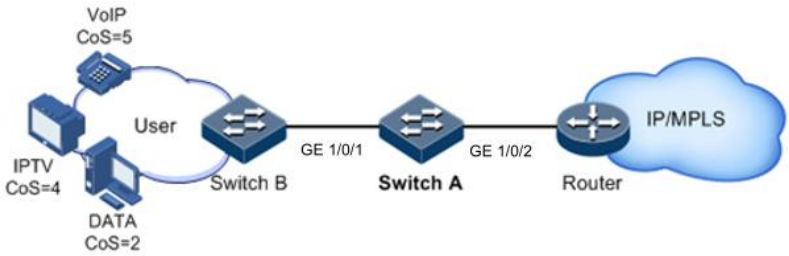
如下图所示，来自 User 的业务类型有语音、视频和数据。

语音业务的 CoS 优先级为 5，视频业务的 CoS 优先级为 4，数据业务的 CoS 优先级为 2。

在 Switch A 处容易发生拥塞，为了减轻网络拥塞造成的影响，根据不同的业务类型，需要制定如下规则：

- 对于语音业务，需要对其进行 SP 调度，优先保证这部分流量通过；
- 对于视频业务，需要对其进行 WRR 调度，权重值为 50；
- 对于数据业务，需要对其进行 WRR 调度，权重值为 20。

图 5-5 配置队列调度组网示意图



配置步骤

步骤 1 配置接口报文根据 8021p 映射内部优先级。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#trust 8021p outer
```

步骤 2 配置在 GE 1/0/2 出方向进行 SP+WRR 队列调度。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#queue scheduling sp+wrr queue 5
SwitchA(config-ge-1/0/2)#queue 4 weight 50
SwitchA(config-ge-1/0/2)#queue 2 weight 20
SwitchA(config-ge-1/0/2)#quit
```

检查结果

查看接口优先级信任模式。

```
JX#show queue interface ge 1/0/2
  Current scheduling algorithm is 'sp+wrr',queue list 5
  'Max-BW' means 'Max Bandwidth'
  'Min-BW' means 'Min Bandwidth'
  Interface     Queue  Max-BW       Min-BW       Weight
```

```
-------------------------------------------------------------------
  ge-1/0/2      0     0M          0M          1
  ge-1/0/2      1     0M          0M          1
  ge-1/0/2      2     0M          0M          20
  ge-1/0/2      3     0M          0M          1
  ge-1/0/2      4     0M          0M          50
  ge-1/0/2      5     0M          0M          --
  ge-1/0/2      6     0M          0M          1
  ge-1/0/2      7     0M          0M          1
-------------------------------------------------------------------
```

5.4 拥塞避免

5.4.1 简介

拥塞避免（Congestion Avoidance）是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞发生或有加剧的趋势时主动丢弃报文，通过调整网络的流量来解除网络过载的一种流量控制机制。

传统的丢包策略采用尾部丢弃（Tail-Drop）的方法，同等的对待所有的报文，不对服务等级进行区分。在拥塞发生期间，队列尾部的数据包将被丢弃，直到拥塞解决。

这种丢弃策略会引发 TCP 全局同步现象，使网络流量忽大忽小，影响链路利用率。

RED

RED（Random Early Detection，随机早期检测）技术通过随机地丢弃报文，让多个 TCP 连接不同时降低发送速度，从而避免了 TCP 的全局同步现象。

在 RED 技术的算法中，为每个队列的长度都设定了阈值上下限，并规定：

- 当队列的长度小于阈值下限时，不丢弃报文。
- 当队列的长度大于阈值上限时，丢弃所有收到的报文。
- 当队列的长度在阈值上限和阈值下限之间时，随机丢弃到来的报文。队列越长，报文被丢弃的概率越高。

WRED

加权随机早期检测 WRED（Weighted Random Early Detection）技术也是通过随机丢弃报文来避免 TCP 的全局同步现象，但该技术生成的随机丢弃参数是基于队列的优先级，它可以依据报文的不同颜色来区别丢弃策略，考虑了高优先级报文的利益并使其被丢弃的概率相对较小。

5.4.2 配置准备

场景

为避免网络拥塞的发生，解决 TCP 全局同步的问题，可以通过配置拥塞避免，调整网络流量，解除网络过载。

前提

5.4.3 拥塞避免的缺省配置

设备上拥塞避免的缺省配置如下。

功能	缺省值
接口 WRED 功能状态	不使能

5.4.4 配置 WRED

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**drop-profile** *drop-profile-name*	创建 WRED 模板，并进入 WRED 配置模式。
3	JX(config-drop-profile)#**color** { **green** | **non-tcp** | **red** | **yellow** } **low-threshold** { *low-threshold-percentage* | **default** } **high-threshold** { *high-threshold-percentage* | **default** } **discard-percentage** { *discard-percentage* | **default** }	{ green | non-tcp | red | yellow }:设置针对绿色/非 TCP/红色/黄色报文的 WRED 参数 low-threshold-percentag :WRED 丢弃的低门限百分比，即 WRED 丢弃的低门限值占队列长度的百分比。 high-threshold-percentage :WRED 丢弃的高门限值百分比，即 WRED 丢弃的高门限值占队列长度的百分比。 discard-percentage :WRED 的最大丢弃概率 缺省情况下，WRED 丢弃模板的高低门限百分比以及最大丢弃概率的取值均为 100
4	JX(config)#**interface** *interface-type interface-number*	进入二层物理层接口配置模式或聚合组接口配置模式。以下步骤以二层物理接口配置模式为例。
5	JX(config-ge-1/0/1)#**qos wred** *drop-profile-name*	配置接口上应用 WRED 模板。
6	JX(config-ge-1/0/1)#**qos queue** *queue-index* **wred** *drop-profile-name*	在接口队列下应用丢弃模版 queue-index 接口队列号 0-7 对应 BE AF1 AF2 AF3 AF4 EF CS6 CS7 drop-profile-name 应用的丢弃模板名称

5.4.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show drop-profile { all | *name* }**	查看 WRED 模板信息。

5.5 流量限速

5.5.1 简介

设备基于流策略对报文流量进行限速外，还支持基于接口、基于 VLAN、基于接口+VLAN 对报文流量进行限速。与基于流策略的流量限速类似，设备对超出部分流量采取丢弃措施。

5.5.2 配置准备

场景

为避免网络发生拥塞或缓解网络拥塞状况，用户可以配置基于接口的流量限速。通过限制某一接口的突发流量，使之以比较均匀的速率发送。

前提

无

5.5.3 配置基于物理接口的流量限速

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**rate-limit { ingress | egress } { gbps | kbps | mbps | percent }** *cir-value*	配置入方向或出方向基于接口的流量限速。

说明

- 缺省情况下，未配置接口的带宽限制。
- 入接口限速资源超过设定的限速值后的处理方式 drop 丢弃。
- 出接口的限速丢包会统计到入接口的丢包统计上。

5.5.4 配置基于接口的流量限速示例

组网需求

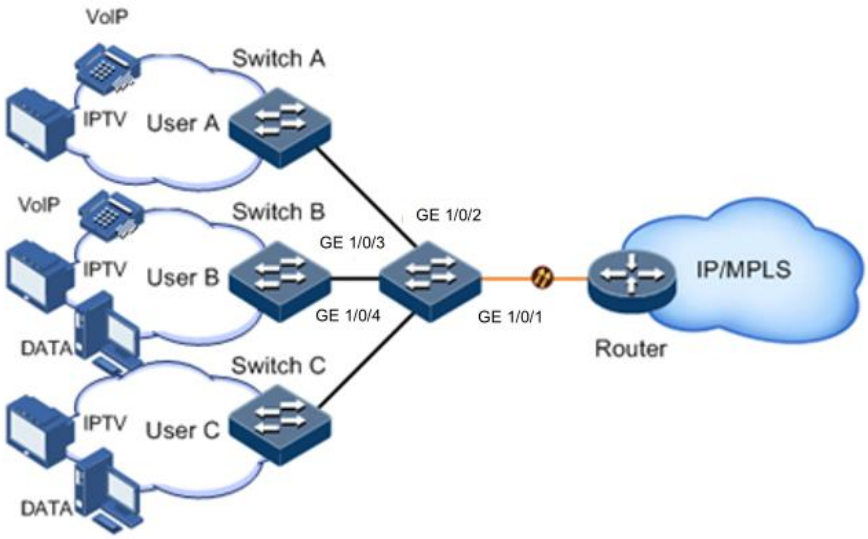
如图 5-5 所示，User A、User B、User C 分别通过 Switch A、Switch B、Switch C 和交换机相连。

来自 User A 的业务类型有语音和视频，来自 User B 的业务类型有语音、视频和数据，来自 User C 的业务类型有视频和数据。

根据各用户的业务需求，需要制定如下规则：

- 对于 User A，须为其提供保证带宽 25M，丢弃多余的流量；
- 对于 User B，须为其提供保证带宽 35M，丢弃多余的流量；
- 对于 User C，须为其提供保证带宽 30M，丢弃多余的流量。

图 5-6 配置基于接口的流量限速组网示意图



配置步骤

步骤 1 配置基于接口的流量限速。

```
JX#config
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#rate-limit in kbps 25000
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#rate-limit in kbps 35000
JX(config-ge-1/0/2)#exit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#rate-limit in kbps 30000
JX(config-ge-1/0/3)#exit
```

6 组播

本章介绍了组播特性的原理和配置过程，并提供相关的配置案例。

- 组播概述
- IGMP Snooping
- MLD Snooping

6.1 组播概述

随着 Internet 网络的不断发展，一方面网络中交互的各种数据、语音和视频信息越来越多；另一方面新兴的电子商务、网上会议、网上拍卖、视频点播、远程教学等服务逐渐兴起，这些服务对网络带宽、信息安全性和有偿性提出了更高的要求。传统的单播和广播方式无法很好的满足这些要求，组播及时满足了这些需求。

组播（Multicast）是一种点到多点的数据传输方式。组播技术能够有效地解决单点发送，多点接收的问题，在网络数据传输时，能够节约网络资源，提高信息安全性。

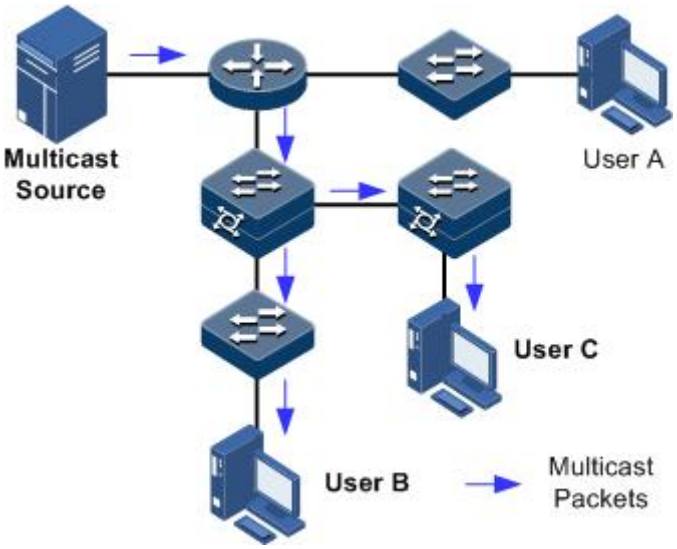
三种通信方式的比较

组播是与单播、广播并列的通信方式：

- 单播方式：系统为每个需要信息的用户单独建立一条数据传送通路，并为该用户发送一份独立的拷贝信息。利用单播方式，网络中传输的信息量和需要该信息的用户量成正比，因此当需要该信息的用户量庞大时，网络中将出现多份相同信息。此时，带宽将成为重要瓶颈，单播方式不利于信息规模化发送。
- 广播方式：系统把信息传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。利用广播方式，信息源将把信息传递给网段中所有用户，用户信息安全性和有偿服务得不到保障。另外，当同一网络中需要该信息的用户量很小时，网络资源利用率将非常低，带宽浪费严重。
- 组播方式：当网络中的某些用户需求特定信息时，组播信息发送者仅发送一份信息，被传递的信息在尽可能远的分叉路口才开始复制和分发。

组播方式传输如下图所示。假设用户 B、C 需要信息，采用组播方式传输，将用户 B、C 组成一个接收者集合，信息源只需发送一份信息，由网络中各交换机根据 IGMP 报文建立自己的组播转发表，信息只传输给实际需要的接收者 B、C。

图 6-1 组播方式传输信息示意图



综上所述，单播方式适合用户稀少的网络，广播方式适合用户稠密的网络，当网络中需要某信息的用户量不确定时，单播和广播方式效率很低。组播方式传输，用户数量成倍增长时，主干带宽不需要随之增加，而且只将信息传递给需要的用户，这些优点使它成为当前网络技术中的研究热点之一。

组播优势与应用

与单播和广播通信方式相比，组播的优势主要在于：

- 提高效率：降低网络流量，减轻了服务器和 CPU 负荷。
- 优化性能：减少冗余量，保障了信息的安全性。
- 分布式应用：解决了点到多点数据传输问题。

组播技术主要应用在以下几个方面：

- 多媒体、流媒体的应用，如：网络电视、网络电台、实时视/音频会议。
- 培训、联合作业场合的通信，如：远程教育、远程医疗。
- 数据仓库、金融应用（股票）。
- 其它任何“点到多点”的应用。

组播中的基本概念

介绍组播中的基本概念：

- 组播组

组播组是指使用一个 IP 组播地址标识的接收者集合。任何用户主机（或其他接收设备）加入一个组播组，就成为了该组成员，可以识别并接收以该 IP 组播地址为目的地址的组播数据。

- 组播组成员

所有加入某组播组的主机便成为该组播组的成员。组播组中的成员是动态的，主机可以在任何时刻加入或离开组播组。组成员可能广泛分布在网络中的任何地方。

- 组播源

以组播组地址为目的地址，发送 IP 报文的信源称为组播源。一个组播源可以同时向多个组播组发送数据，多个组播源可以同时向一个组播组发送数据。

- 组播路由器

在组播传输中提供三层组播功能的路由器。组播路由器能够实现组播路由，指导组播报文转发，也能够在与用户连接的末梢网段上提供组播组成员管理功能。

- 路由器接口

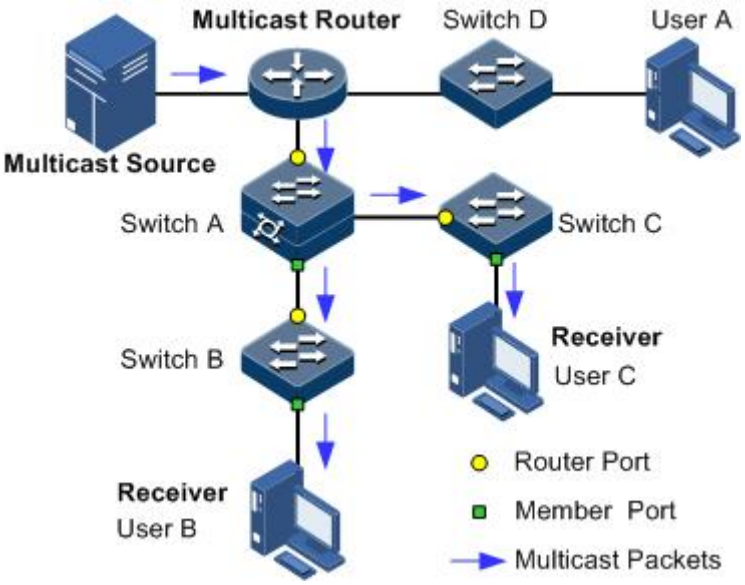
是指组播路由器和主机之间的设备上，朝向组播路由器的接口，设备从该接口接收组播报文。

- 成员接口

也称接收接口，是指组播路由器和主机之间的设备上，朝向主机的接口，设备从该接口发出组播报文。

组播基本概念中路由器接口，成员接口位置标示如下图所示。

图 6-2 组播基本概念在网络中相应位置标示示意图



组播地址

为了让组播源和组播组成员进行通信，需要提供网络层组播地址和链路层组播地址，即 IP 组播地址和组播 MAC 地址。需要注意的是组播地址都只能作为目的地址，而不能作为源地址来使用。

- IP 组播地址

IANA（Internet Assigned Numbers Authority，互联网编号分配委员会）将 D 类地址空间分配给 IPv4 组播使用，IPv4 组播地址范围 224.0.0.0～239.255.255.255。

- 组播 MAC 地址

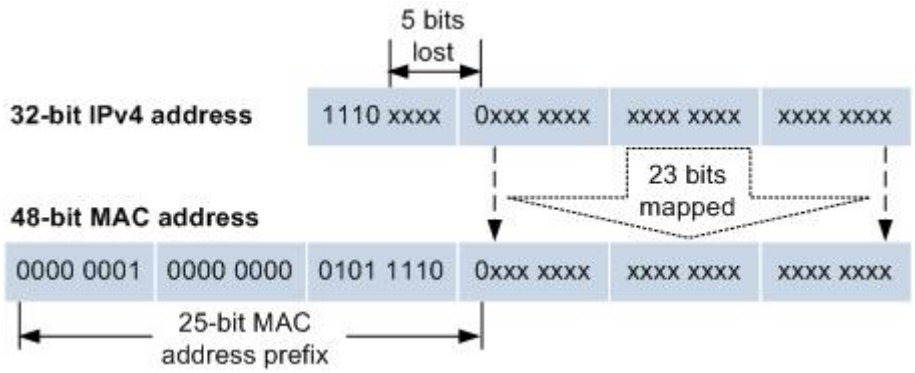
以太网传输单播 IP 报文时，目的 MAC 地址使用的是接收者的 MAC 地址。但是在传输组播数据包时，其目的地不再是一个具体的接收者，而是一个成员不确定的组，所以要使用组播 MAC 地址。

组播 MAC 地址用于在链路层上标识属于同一组播组的接收者。

IANA 规定，组播 MAC 地址的高 24 位为 0x01005E，第 25 位为 0，低 23 位为 IPv4 组播地址的低 23 位。

IP 组播地址和 MAC 地址以一种映射关系相关联，映射关系如下图所示。

图 6-3 IPv4 组播地址和组播 MAC 地址的映射关系



由于 IP 组播地址的前 4 位是 1110，代表组播标识，而后 28 位中只有 23 位被映射到 MAC 地址，这样 IP 地址中就有 5 位信息丢失，可能导致 32 个 IP 组播地址映射到同一 MAC 地址上。因此在二层处理过程中，设备可能要接收一些本 IPv4 组播组以外的组播数据，而这些多余的组播数据就需要设备的上层进行过滤了。

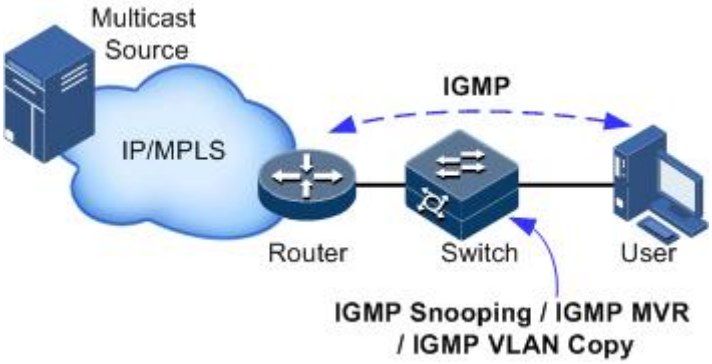
组播协议基础

实现一套完整的组播服务，需要在网络各个位置部署多种组播协议相互配合，共同运作。

通常，把工作在网络层的 IP 组播称为“三层组播”，相应的组播协议称为“三层组播协议”，包括 IGMP（Internet Group Management Protocol，因特网组管理协议）等；把工作在数据链路层的 IP 组播称为“二层组播”，相应的组播协议称为“二层组播协议”，包括 IGMP Snooping（Internet Group Management Protocol Snooping，因特网组管理协议监听）等。

IGMP 和二层组播特性运行位置如下图所示。

图 6-4 IGMP 和二层组播特性运行位置示意图



IGMP 是 TCP/IP 协议族中负责 IPv4 组播成员管理的协议。IGMP 运行在组播路由器和主机之间，该协议定义了主机与组播路由器之间建立、维护组播组成员关系的机制。IGMP 不包括组播路由器之间的组成员关系信息的传播与维护，这部分工作由组播路由协议完成。

IGMP 通过在主机和组播路由器之间交互 IGMP 报文实现组成员管理功能。IGMP 报文封装在 IP 报文中，IGMP 报文类型有 Query 查询报文、Report 报告报文和 Leave 离开报文。IGMP 基本功能：

- 主机发送 Report 报文加入组播组，发送 Leave 报文离开组播组，自主决定接收哪些组播组的报文。
- 组播路由器周期发送 Query 报文，并接收主机反馈的 Report 报文和 Leave 报文，了解连接的网段上有哪些组播组成员。如果有组播组成员，应将组播数据转发到这个网段；如果没有组播组成员则不转发。

到目前为止，IGMP 有三个版本：IGMPv1 版本、IGMPv2 版本和 IGMPv3 版本，新版本完全兼容旧版本。目前应用最广泛的是 IGMPv2，其中 Leave 报文 IGMPv1 版本不支持。

二层组播运行在主机和组播路由器之间的二层设备上。

二层组播通过监听和分析主机和组播路由器之间交互的 IGMP 报文来管理和控制组播组，实现组播数据在二层的转发，抑制组播数据在二层网络中的扩散。

二层组播基础

二层组播基础功能包含：

- 指定组播路由器接口；
- 使能立即离开功能；
- 设置组播转发表项和路由器接口的老化时间；

与二层组播基础功能有关的概念说明。

- 组播路由器接口

在运行组播功能的二层交换机上，可以动态学习（需要在组播路由器上开启组播路由协议，通过组播 Query 报文学习）到路由器接口，也可以手工设置，以使下游的组播报告、离开等报文可以转发到该路由器接口。

动态学习到的路由器接口有老化时间，手工配置的路由器接口不会老化。

- 老化时间

设置的老化时间同时作用于组播转发表项的老化时间和路由器接口的老化时间。

在运行组播功能的二层交换机上，每个动态学习到的路由器接口会启动一个定时器。到达老化时间时未收到 Query 报文，该路由器接口将被删除；收到 Query 报文时，更新路由器接口的超时时间。

每条组播转发表项会启动一个定时器，也就是组播成员的老化时间，到达老化时间时未收到 Report 报文，该组播成员将会被删除；收到 Report 报文时，更新组播转发表项的超时时间。

- 立即离开功能

在运行组播功能的二层交换机上，当用户发送 Leave 报文时，并不立即删除对应的组播转发表项，而是等待表项老化时才删除。当下游用户数量较多，并且加入离开比较频繁时，可以打开此功能，这样对应的组播转发表项被快速删除。

6.2 IGMP Snooping

6.2.1 简介

IGMP Snooping 是运行在二层设备上的组播约束机制，用于管理和控制组播组，实现二层组播。

IGMP Snooping 允许交换机监听主机和组播路由器之间的 IGMP 会话。当交换机监听到主机发往某个组的 IGMP Report，交换机将主机所在的接口加入到这个组的转发列表中，同样，当转发表项达到老化时间时，就将主机所在的接口从转发表中删除。

IGMP Snooping 利用二层组播转发表进行组播数据转发，当交换机收到组播数据时，会直接根据组播转发表项的相应的接收接口进行转发，并不向所有接口洪泛，因此有效地节省了交换机的带宽。

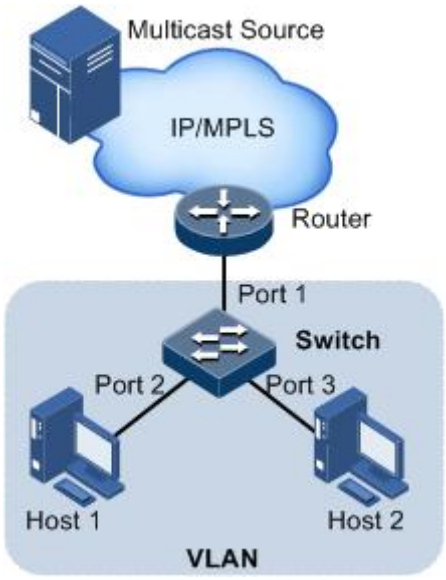
IGMP Snooping 建立二层组播转发表，可以通过 IGMP Snooping 动态学习，也可以进行手工配置。

6.2.2 配置准备

场景

如下图所示，多个主机接收组播源的数据，多个主机属于同一个 VLAN。可以在组播路由器和主机相连的交换机上运行 IGMP Snooping，通过监听组播路由器和主机之间的 IGMP 报文，建立和维护组播转发表，实现二层组播。

图 6-5 IGMP Snooping 应用场景



前提

在配置 IGMP Snooping 之前，需完成以下任务：

- 创建 VLAN，并将相应接口加入 VLAN。

6.2.3 IGMP Snooping 的缺省配置

设备上 IGMP Snooping 的缺省配置如下。

功能	缺省值
全局 IGMP Snooping 状态	禁用
VLAN 的 IGMP Snooping 状态	禁用
接口的 IGMP Snooping 状态	禁用
IGMP Snooping 协议版本	v2
通用查询间隔	60s
健壮系数	2
最大响应时间	10s
路由器端口老化时间	180s
接口的最大组播组限制	1000

6.2.4 配置 IGMP Snooping 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**igmp-snooping start**	全局使能 IGMP Snooping。
3	JX(config)#**igmp-snooping router-aging-time** *aging-time*	（可选）配置路由器端口老化时间
4	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
5	JX(config-vlan-10)#**igmp-snooping enable**	VLAN 使能 IGMP Snooping
6	JX(config-vlan-10)#**igmp-snooping version** { **v1** | **v2** | **V3** }	（可选）配置协议版本
7	JX(config-vlan-10)#**igmp-snooping forwarding-mode** { **ip** | **mac** }	（可选）配置组播表项转发模式 基于组播 ip 或者基于组播 mac
8	JX(config-vlan-10)#**igmp-snooping require-router-alert enable**	（可选）配置 Router-Alert 选项检查
9	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
10	JX(config-ge-1/0/1)#**igmp-snooping enable**	接口使能 IGMP Snooping
11	JX(config-vlan-10)#**igmp-snooping 8021p priorit** { **default** | *priority* }	（可选）配置 igmp vlan 的 8021P 权重值

6.2.5 配置 IGMP Snooping 查询器功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**igmp-snooping query-interval** *interval*	（可选）配置通用查询间隔。
3	JX(config)#**igmp-snooping robust-count** *count*	（可选）配置健壮系数
4	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
5	JX(config-vlan-10)#**igmp-snooping querier enable**	配置查询器使能 使能了查询器才会发送通用查询和特定组查询

6	JX(config-vlan-10)#**igmp-snooping send-query source-address** *ip-address*	（可选）配置设备发送查询报文的源 IP 地址
7	JX(config-vlan-10)#**igmp-snooping max-response-time** *response-time*	（可选）配置查询报文最大响应时间
8	JX(config-vlan-10)#**igmp-snooping lastmember-queryinterval** *interval*	（可选）配置特定组查询报文发送间隔
9	JX(config-vlan-10)#**igmp-snooping lastmember-querynumber** *number*	（可选）配置特定组查询报文发送个数

6.2.6 配置 IGMP Snooping 报文抑制功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
4	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
8	JX(config-vlan-10)#**igmp-snooping report-suppres enable**	配置 Report 和 Leave 报文抑制

6.2.7 配置 IGMP Snooping 组播复制功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
3	JX(config-vlan-10)#**igmp-snooping forwarding-mode ip**	配置转发模式为 IP 模式
4	JX(config-vlan-10)#**igmp-snooping multicast-duplicate enable**	配置组播复制使能
5	JX(config-vlan-10)#**igmp-snooping multicast user-vlan** *VLANLIST*	配置组播复制关联的用户 VLAN

6.2.8 配置 IGMP Snooping 静态组播成员功能

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**igmp-snooping static-group group-address** *group-address* [**source-address** *source-address*] **vlan** *vlan-id* [**user-vlan** *vlan-list*]	配置接口为静态组播成员

说明

1. 如果需要配置 source-address 的静态组播成员，需要协议版本配置为 v3。
2. 如果需要配置 user-vlan，需要使能组播复制

6.2.9 配置 IGMP Snooping Proxy 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
3	JX(config-vlan-10)#**igmp-snooping workmode igmp-proxy**	配置工作模式为 Proxy 模式
4	JX(config-vlan-10)#**igmp-snooping querier enable**	配置查询器使能 Proxy 模式必须打开查询器，否则组播表项可能会老化
5	JX(config-vlan-10)#**igmp-snooping proxy-ip** *ip-address*	（可选）配置 Proxy 模式的代理 IP 地址

6.2.10 配置 IGMP Snooping 接口组播组个数限制

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**igmp-snooping group-limit** *number* [**action** { **delay** | **replace** }]	配置接口组播组限制个数。

6.2.11 配置 IGMP Snooping 组播策略

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**acl-ipv4** *list-id* JX(configure-acl-ipv4-*)#**rule** *rule-id* **src-ip any dst-ip** *dst-ip-address/ dst-ip-mask* JX(configure-acl-ipv4-*)#**rule** *rule-id* **action** { **permit** | **deny** }	创建并配置 ACL 策略模板 策略只保护对目的 IP 地址的 permit 和 deny
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
4	JX(config-ge-1/0/1)#**igmp-snooping group-policy acl-ipv4** *list-id*	接口组播策略绑定 ACL 模板
5	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
6	JX(config-vlan-10)#**igmp-snooping group-policy acl-ipv4** *list-id*	VLAN 组播策略绑定 ACL 模板

说明

VLAN 和接口同时配置组播策略时，如果 VLAN 的策略为 deny 则不再检查接口的策略。

6.2.12 配置 IGMP Snooping SSM Mapping 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**acl-ipv4** *list-id* JX(configure-acl-ipv4-*)#**rule** *rule-id* **src-ip any dst-ip** *dst-ip-address/ dst-ip-mask* JX(configure-acl-ipv4-*)#**rule** *rule-id* **action** { **permit** | **deny** }	创建并配置 ACL 策略模板 策略只保护对目的 IP 地址的 permit 和 deny
3	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
4	JX(config-vlan-10)#**igmp-snooping forwarding-mode ip**	配置转发模式为 IP 模式
5	JX(config-vlan-10)#**igmp-snooping version v3**	配置协议版本为 v3

6	JX(config-vlan-10)#**igmp-snooping ssm-mapping enable**	使能 SSM Mapping 功能
7	JX(config-vlan-10)#**igmp-snooping ssm-mapping acl-ipv4** *list-id* **source-addres** *ip-address*	配置组地址与源地址的映射 ACL 动作为 permit 的组地址进行映射

6.2.13 配置 IGMP Snooping 静态路由端口配置

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	进入 vlan 配置模式。
3	JX(config-vlan-10)#**igmp-snooping router-port** *interface-type interface-number*	配置静态路由端口。
4	JX(config-vlan-10)#**igmp-snooping router-port drop-report** { **enable** | **disable** }	配置静态路由端口丢弃报告包。
5	JX(config-vlan-10)#**igmp-snooping router-port-limit** { **default** | *value* }	配置静态路由端口数量限制。

6.2.14 检查配置

配置完成后，请在设备上进行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show igmp-snooping config**	查看 IGMP Snooping 配置信息。
2	JX#**show igmp-snooping interface**	查看 IGMP Snooping 接口信息
3	JX#**show igmp-snooping vlan**	查看 IGMP Snooping 组播 VLAN 信息
4	JX#**show igmp-snooping forwarding-table**	查看 IGMP Snooping 组播转发表项

6.2.15 维护

用户可以通过以下命令维护 IGMP Snooping。

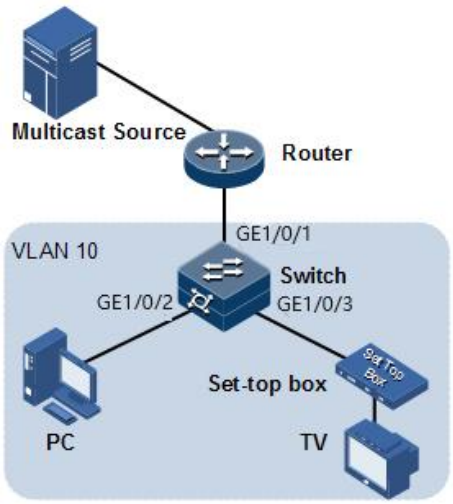
命令	描述
JX(config)#**reset igmp-snooping forwarding-table**	清除动态学习的组播转发表项。
JX(config)#**reset igmp-snooping statistics**	清除 IGMP Snooping 协议报文统计。

6.2.16 配置 IGMP Snooping 基本功能应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 IGMP Snooping 功能

图 6-6 IGMP Snooping 基本功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 IGMP Snooping。

```
JX(config)#igmp-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#igmp-snooping enable
JX(config-vlan-10)#quit
```

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#igmp-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#igmp-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#igmp-snooping enable
JX(config-ge-1/0/3)#quit
```

检查结果

查看 IGMP Snooping 配置信息是否正确。

```
JX#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
 igmp-snooping enable
!
interface ge 1/0/1
 igmp-snooping enable
!
interface ge 1/0/2
 igmp-snooping enable
!
interface ge 1/0/3
 igmp-snooping enable
```

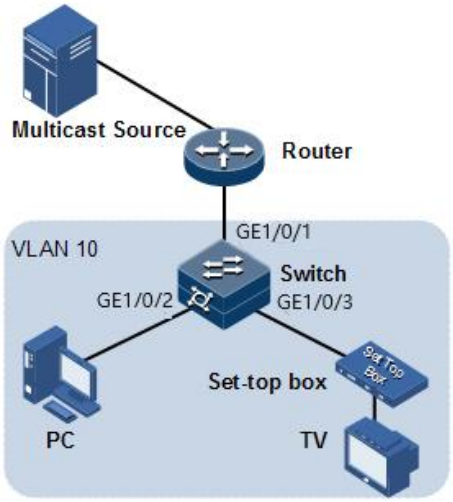
6.2.17 配置 IGMP Snooping 静态成员应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 IGMP Snooping 功能

其中 Gigaethernet 1/0/2 下用户希望长期稳定接收 225.1.1.1 ~ 225.1.1.3 的组播数据。

图 6-7 IGMP Snooping 静态成员功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 IGMP Snooping。

```
JX(config)#igmp-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#igmp-snooping enable
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#igmp-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#igmp-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#igmp-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置 IGMP Snooping 静态组播成员

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/1)#igmp-snooping static-group group-address 225.1.1.1
vlan 10
JX(config-ge-1/0/1)#igmp-snooping static-group group-address 225.1.1.2
vlan 10
JX(config-ge-1/0/1)#igmp-snooping static-group group-address 225.1.1.3
vlan 10
```

检查结果

查看 IGMP Snooping 配置信息是否正确。

```
JX#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
 igmp-snooping enable
!
interface ge 1/0/1
 igmp-snooping enable
!
interface ge 1/0/2
 igmp-snooping enable
 igmp-snooping static-group group-address 225.1.1.1 vlan 10
 igmp-snooping static-group group-address 225.1.1.2 vlan 10
 igmp-snooping static-group group-address 225.1.1.3 vlan 10
!
interface ge 1/0/3
 igmp-snooping enable
```

查看 IGMP Snooping 静态转发表是否正确

```
JX#show igmp-snooping forwarding-table
 S:Static,  D:dynamic,   E:Exclude,   I:Include
 Vlan     (Source,Group)             Port         OutVlan       Flag
Expires
 10       (*,225.1.1.1)              ge-1/0/2      10           S/E      --
 10       (*,225.1.1.2)              ge-1/0/2      10           S/E      --
 10       (*,225.1.1.3)              ge-1/0/2      10           S/E      --
 Total Group Number: 3
```

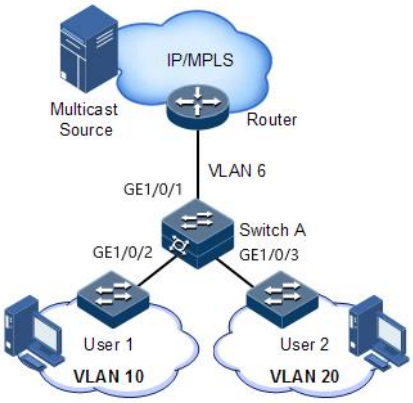
6.2.18 配置 IGMP Snooping 组播复制应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，组播 VLAN 和用户 VLAN 不同，配置 IGMP Snooping 组播复制功能，

其中 GE1/0/1 加入组播 VLAN 6， 用户 1 加入用户 VLAN 10，用户 2 加入 VLAN 20。

图 6-8 IGMP Snooping 组播复制功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 6,10,20
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 6
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 20
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 IGMP Snooping 功能

```
JX(config)#igmp-snooping start
JX(config)#vlan 6
JX(config-vlan-6)#igmp-snooping enable
JX(config-vlan-6)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#igmp-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#igmp-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#igmp-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置使能 IGMP Snooping 开启组播复制功能

```
JX(config)#vlan 6
JX(config-vlan-6)#igmp-snooping forwarding-mode ip
```

```
JX(config-vlan-6)#igmp-snooping multicast-duplicate enable
JX(config-vlan-6)#igmp-snooping multicast user-vlan 10,20
JX(config-vlan-6)#quit
```

检查结果

查看 IGMP Snooping 配置信息是否正确。

```
JX#show igmp-snooping config
!
igmp-snooping start
!
vlan 6
 igmp-snooping enable
 igmp-snooping forwarding-mode ip
 igmp-snooping multicast-duplicate enable
 igmp-snooping multicast user-vlan 10,20
!
interface ge 1/0/1
 igmp-snooping enable
!
interface ge 1/0/2
 igmp-snooping enable
!
interface ge 1/0/3
 igmp-snooping enable
```

6.2.19 配置 IGMP Snooping Proxy 应用示例

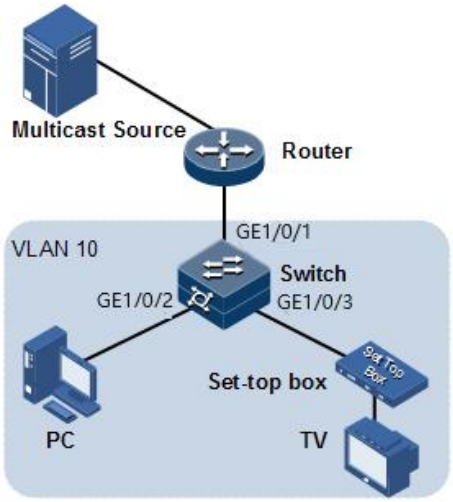
组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 IGMP Snooping 功能

在交换机上开启 IGMP Proxy 功能，减少主机和组播路由器之间的通信，同时又不影响组播功能实现。

图中 PC 和机顶盒加入同一个组播组时，交换机收到两份 IGMP Report 报文，只向组播路由器发送一份 IGMP Report 报文。组播路由器发送的 IGMP Query 报文不再向下游转发，而是由交换机定时发送 IGMP Query 报文。

图 6-9 IGMP Snooping Proxy 功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 IGMP Snooping 功能

```
JX(config)#igmp-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#igmp-snooping enable
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#igmp-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#igmp-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#igmp-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置使能 IGMP Snooping 开启 IGMP Proxy 功能

```
JX(config)#vlan 10
JX(config-vlan-10)#igmp-snooping workmode igmp-proxy
JX(config-vlan-10)#igmp-snooping querier enable
JX(config-vlan-10)#quit
```

检查结果

查看 IGMP Snooping 配置信息是否正确。

```
JX#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
 igmp-snooping enable
 igmp-snooping workmode igmp-proxy
 igmp-snooping querier enable
!
interface ge 1/0/1
 igmp-snooping enable
!
interface ge 1/0/2
 igmp-snooping enable
!
interface ge 1/0/3
 igmp-snooping enable
```

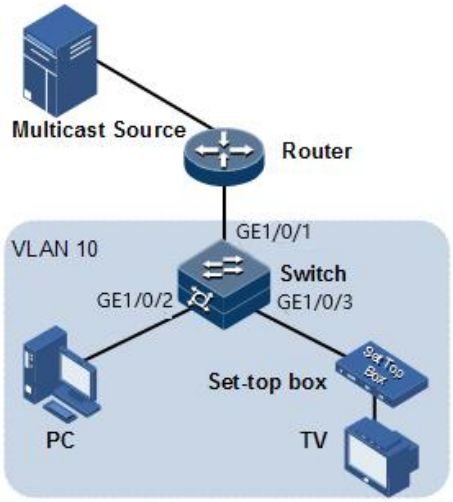
6.2.20 配置 IGMP Snooping 策略应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 IGMP Snooping 功能

在交换机上开启组播策略功能，接口 Gigaethernet 1/0/2 的用户允许加入 225.1.1.1 ~ 225.1.1.3，接口 Gigaethernet 1/0/3 的用户允许加入 225.1.1.4 ~ 225.1.1.6。

图 6-10 IGMP Snooping 组播策略功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 IGMP Snooping 功能

```
JX(config)#igmp-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#igmp-snooping enable
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#igmp-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#igmp-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#igmp-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置 GE1/0/2 用户的 ACL 模板

```
JX(config)#acl-ipv4 1001
JX(configure-acl-ipv4-1001)#rule 1 src-ip any dst-ip 225.1.1.1/32
JX(configure-acl-ipv4-1001)#rule 1 action permit
JX(configure-acl-ipv4-1001)#rule 2 src-ip any dst-ip 225.1.1.2/32
JX(configure-acl-ipv4-1001)#rule 2 action permit
JX(configure-acl-ipv4-1001)#rule 3 src-ip any dst-ip 225.1.1.3/32
JX(configure-acl-ipv4-1001)#rule 3 action permit
JX(configure-acl-ipv4-1001)#quit
```

步骤 4 配置 GE1/0/3 用户的 ACL 模板

```
JX(config)#acl-ipv4 1002
JX(configure-acl-ipv4-1002)#rule 1 src-ip any dst-ip 225.1.1.4/32
JX(configure-acl-ipv4-1002)#rule 1 action permit
JX(configure-acl-ipv4-1002)#rule 2 src-ip any dst-ip 225.1.1.5/32
JX(configure-acl-ipv4-1002)#rule 2 action permit
JX(configure-acl-ipv4-1002)#rule 3 src-ip any dst-ip 225.1.1.6/32
JX(configure-acl-ipv4-1002)#rule 3 action permit
JX(configure-acl-ipv4-1002)#quit
```

步骤 5 配置接口绑定组播策略 ACL 模板

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#igmp-snooping group-policy acl-ipv4 1001
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#igmp-snooping group-policy acl-ipv4 1002
JX(config-ge-1/0/3)#quit
```

检查结果

查看 IGMP Snooping 配置信息是否正确。

```
JX#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
 igmp-snooping enable
!
interface ge 1/0/2
 igmp-snooping enable
 igmp-snooping group-policy acl-ipv4 1001 version 1-3
!
interface ge 1/0/3
 igmp-snooping enable
 igmp-snooping group-policy acl-ipv4 1002 version 1-3
```

查看 ACL 模板配置是否正确。

```
JX#show acl config
!
acl-ipv4 1001
 rule 1 src-ip any dst-ip 225.1.1.1/32
 rule 1 action permit
 rule 2 src-ip any dst-ip 225.1.1.2/32
 rule 2 action permit
```

```
 rule 3 src-ip any dst-ip 225.1.1.3/32
 rule 3 action permit
acl-ipv4 1002
 rule 1 src-ip any dst-ip 225.1.1.4/32
 rule 1 action permit
 rule 2 src-ip any dst-ip 225.1.1.5/32
 rule 2 action permit
 rule 3 src-ip any dst-ip 225.1.1.6/32
 rule 3 action permit
```

6.3 MLD Snooping

6.3.1 简介

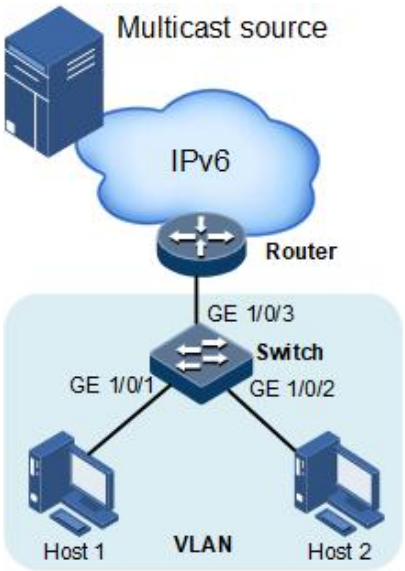
MLD Snooping 是一种 IPv6 二层组播协议，该协议侦听三层组播设备和用户主机之间发送的组播协议报文，维护组播报文出端口的信息，进而管理和控制组播数据报文的转发。

6.3.2 配置准备

场景

多个主机接收组播源的数据，多个主机属于同一个 VLAN。可以在组播路由器和主机相连的交换机上运行 MLD Snooping，通过监听组播路由器和主机之间的 MLD 报文，建立和维护组播转发表，实现二层组播。

图 6-11 MLD Snooping 应用场景



前提

在配置 MLD Snooping 之前，需完成以下任务：

- 创建 VLAN，并将相应接口加入 VLAN。

6.3.3 MLD Snooping 的缺省配置

功能	缺省值
全局 MLD Snooping 状态	禁用
VLAN 的 MLD Snooping 状态	禁用
接口的 MLD Snooping 状态	禁用
MLD Snooping 协议版本	v1
通用查询间隔	60s
健壮系数	2
最大响应时间	10s
路由器端口老化时间	180s
接口的最大组播组限制	1000

6.3.4 配置 MLD Snooping 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**mld-snooping start**	全局使能 MLD Snooping。
3	JX(config)#**mld-snooping router-aging-time** *aging-time*	（可选）配置路由器端口老化时间
4	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
5	JX(config-vlan-10)#**mld-snooping enable**	VLAN 使能 MLD Snooping
6	JX(config-vlan-10)#**mld-snooping version** { **v1** | **v2** }	（可选）配置协议版本
7	JX(config-vlan-10)#**mld-snooping forwarding-mode** { **ip** | **mac** }	（可选）配置组播表项转发模式 基于组播 ip 或者基于组播 mac
8	JX(config-vlan-10)#**mld-snooping require-router-alert enable**	（可选）配置 Router-Alert 选项检查

9	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
10	JX(config-ge-1/0/1)#**mld-snooping enable**	接口使能 MLD Snooping

6.3.5 配置 MLD Snooping 查询器功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**mld-snooping query-interval** *interval*	（可选）配置通用查询间隔。
3	JX(config)#**mld-snooping robust-count** *count*	（可选）配置健壮系数
4	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
5	JX(config-vlan-10)#**mld-snooping querier enable**	配置查询器使能 使能了查询器才会发送通用查询和特定组查询
6	JX(config-vlan-10)#**mld-snooping send-query source-address** *ipv6-address*	（可选）配置设备发送查询报文的源 IP 地址
7	JX(config-vlan-10)#**mld-snooping max-response-time** *response-time*	（可选）配置查询报文最大响应时间
8	JX(config-vlan-10)#**mld-snooping lastmember-queryinterval** *interval*	（可选）配置特定组查询报文发送间隔
9	JX(config-vlan-10)#**mld-snooping lastmember-querynumber** *number*	（可选）配置特定组查询报文发送个数

6.3.6 配置 MLD Snooping 报文抑制功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
4	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
8	JX(config-vlan-10)#**mld-snooping report-suppres enable**	配置 Report 和 Leave 报文抑制

6.3.7 配置 MLD Snooping 组播复制功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
3	JX(config-vlan-10)#**mld-snooping forwarding-mode ip**	配置转发模式为 IP 模式
4	JX(config-vlan-10)#**mld-snooping multicast-duplicate enable**	配置组播复制使能
5	JX(config-vlan-10)#**mld-snooping multicast user-vlan** *VLANLIST*	配置组播复制关联的用户 VLAN

6.3.8 配置 MLD Snooping 静态组播成员功能

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**mld-snooping static-group group-address** *group-address* **vlan** *vlan-id* [**user-vlan** *vlan-list*]	配置接口为静态组播成员

说明

1. 如果需要配置 user-vlan，需要使能组播复制

6.3.9 配置 MLD Snooping Proxy 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
3	JX(config-vlan-10)#**mld-snooping workmode mld-proxy**	配置工作模式为 Proxy 模式

4	JX(config-vlan-10)#**mld-snooping querier enable**	配置查询器使能 Proxy 模式必须打开查询器，否则组播表项可能会老化
5	JX(config-vlan-10)#**mld-snooping proxy-ip** *ipv6-address*	（可选）配置 Proxy 模式的代理 IPv6 地址

6.3.10 配置 MLD Snooping 接口组播组个数限制

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**mld-snooping group-limit** *number* [**action** { **delay** | **replace** }]	配置 mld-snooping 的个数限制及超限动作。

6.3.11 配置 MLD Snooping 组播策略

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**acl-ipv6** *list-id* JX(configure-acl-ipv6-*)#**rule** *rule-id* **src-ip any dst-ip** *dst-ip-address/ dst-ip-mask* JX(configure-acl-ipv6-*)#**rule** *rule-id* **action** { **permit** | **deny** }	创建并配置 ACL 策略模板 策略只保护对目的 IPv6 地址的 permit 和 deny
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
4	JX(config-ge-1/0/1)#**mld-snooping group-policy acl-ipv6** *list-id*	接口组播策略绑定 ACL 模板
5	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
6	JX(config-vlan-10)#**mld-snooping group-policy acl-ipv6** *list-id*	VLAN 组播策略绑定 ACL 模板

说明

VLAN 和接口同时配置组播策略时，如果 VLAN 的策略为 deny 则不再检查接口的策略。

6.3.12 配置 MLD Snooping SSM Mapping 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**acl-ipv6** *list-id*	创建并配置 ACL 策略模板 策略只保护对目的 IP 地址的 permit 和 deny
3	JX(config)#**vlan** *vlan-id*	进入 VLAN 配置视图
4	JX(config-vlan-10)#**mld-snooping forwarding-mode ip**	配置转发模式为 IP 模式
5	JX(config-vlan-10)#**mld-snooping version v2**	配置协议版本为 v2
6	JX(config-vlan-10)#**mld-snooping ssm-mapping enable**	使能 SSM Mapping 功能
7	JX(config-vlan-10)#**mld-snooping ssm-mapping acl-ipv6** *list-id* **source-addres** *ipv6-address*	配置组地址与源地址的映射 ACL 动作为 permit 的组地址进行映射

6.3.13 检查配置

配置完成后，请在设备上进行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show mld-snooping config**	查看 MLD Snooping 配置信息。
2	JX#**show mld-snooping interface**	查看 MLD Snooping 接口信息
3	JX#**show mld-snooping vlan**	查看 MLD Snooping 组播 VLAN 信息
4	JX#**show mld-snooping forwarding-table**	查看 MLD Snooping 组播转发表项

6.3.14 维护

用户可以通过以下命令维护 MLD Snooping。

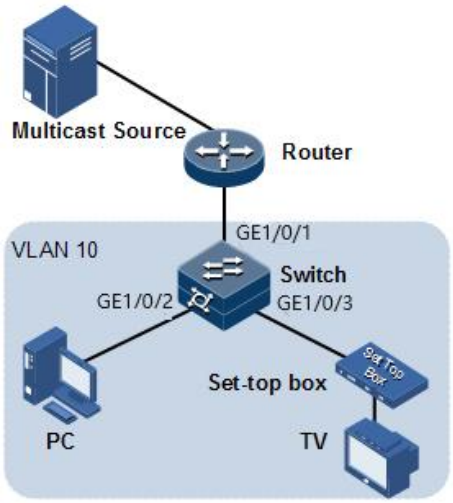
命令	描述
JX(config)#**reset mld-snooping forwarding-table**	清除动态学习的组播转发表项。

6.3.15 配置 MLD Snooping 基本功能应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 MLD Snooping 功能

图 6-12 MLD Snooping 基本功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 MLD Snooping。

```
JX(config)#mld-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#mld-snooping enable
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#mld-snooping enable
```

```
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#mld-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#mld-snooping enable
JX(config-ge-1/0/3)#quit
```

检查结果

查看 MLD Snooping 配置信息是否正确。

```
JX#show mld-snooping config
!
mld-snooping start
!
vlan 10
 mld-snooping enable
!
interface ge 1/0/1
 mld-snooping enable
!
interface ge 1/0/2
 mld-snooping enable
!
interface ge 1/0/3
 mld-snooping enable
```

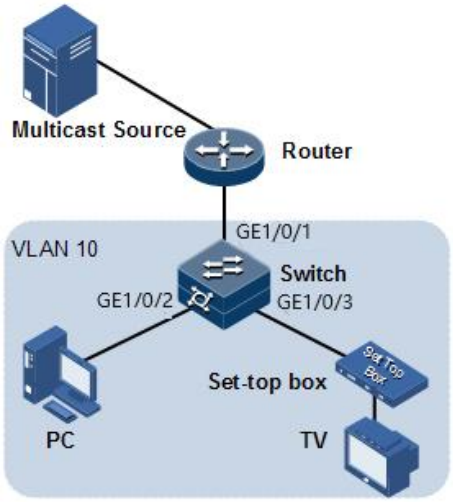
6.3.16 配置 MLD Snooping 静态成员应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 MLD Snooping 功能

其中 Gigaethernet 1/0/2 下用户希望长期稳定接收 ff1e::1 ~ ff1e::3 的组播数据。

图 6-13 MLD Snooping 静态成员功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 MLD Snooping。

```
JX(config)#mld-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#mld-snooping enable
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#mld-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#mld-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#mld-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置 MLD Snooping 静态组播成员

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/1)#mld-snooping static-group group-address ff1e::1 vlan
10
JX(config-ge-1/0/1)#mld-snooping static-group group-address ff1e::2 vlan
10
JX(config-ge-1/0/1)#mld-snooping static-group group-address ff1e::3 vlan
10
```

检查结果

查看 MLD Snooping 配置信息是否正确。

```
JX#show mld-snooping config
!
mld-snooping start
!
vlan 10
 mld-snooping enable
!
interface ge 1/0/1
 mld-snooping enable
 mld-snooping static-group group-address ff1e::1 vlan 10
 mld-snooping static-group group-address ff1e::2 vlan 10
 mld-snooping static-group group-address ff1e::3 vlan 10
!
interface ge 1/0/2
 mld-snooping enable
!
interface ge 1/0/3
 mld-snooping enable
```

查看 MLD Snooping 静态转发表是否正确

```
JX#show mld-snooping forwarding-table
 S:Static,  D:dynamic,   E:Exclude,   I:Include
 Vlan     (Source,Group)         Port         OutVlan       Flag   Expires
-------------------------------------------------------------------------
-----------------------------------
 10       (*,ff1e::1)            ge-1/0/1      10           S/E    --
 10       (*,ff1e::2)            ge-1/0/1      10           S/E    --
 10       (*,ff1e::3)            ge-1/0/1      10           S/E    --
-------------------------------------------------------------------------
-----------------------------------
 Total Group Number: 3
```

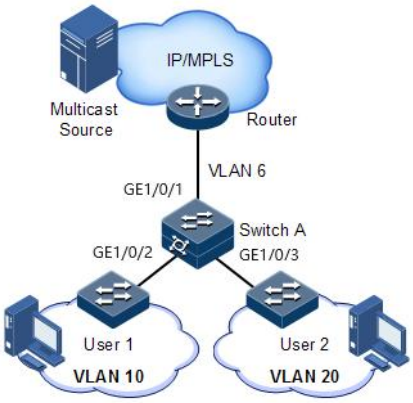
6.3.17 配置 MLD Snooping 组播复制应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，组播 VLAN 和用户 VLAN 不同，配置 MLD Snooping 组播复制功能，

其中 GE1/0/1 加入组播 VLAN 6， 用户 1 加入用户 VLAN 10，用户 2 加入 VLAN 20。

图 6-14 MLD Snooping 组播复制功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 6,10,20
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 6
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 20
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 MLD Snooping 功能

```
JX(config)#mld-snooping start
JX(config)#vlan 6
JX(config-vlan-6)#mld-snooping enable
JX(config-vlan-6)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#mld-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#mld-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#mld-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置使能 MLD Snooping 开启组播复制功能

```
JX(config)#vlan 6
JX(config-vlan-6)#mld-snooping forwarding-mode ip
```

```
JX(config-vlan-6)#mld-snooping multicast-duplicate enable
JX(config-vlan-6)#mld-snooping multicast user-vlan 10,20
JX(config-vlan-6)#quit
```

检查结果

查看 MLD Snooping 配置信息是否正确。

```
JX#show mld-snooping config
!
mld-snooping start
!
vlan 10
 mld-snooping enable
 mld-snooping forwarding-mode ip
 mld-snooping multicast-duplicate enable
 mld-snooping multicast user-vlan 10,20
!
interface ge 1/0/1
 mld-snooping enable
!
interface ge 1/0/2
 mld-snooping enable
!
interface ge 1/0/3
 mld-snooping enable
```

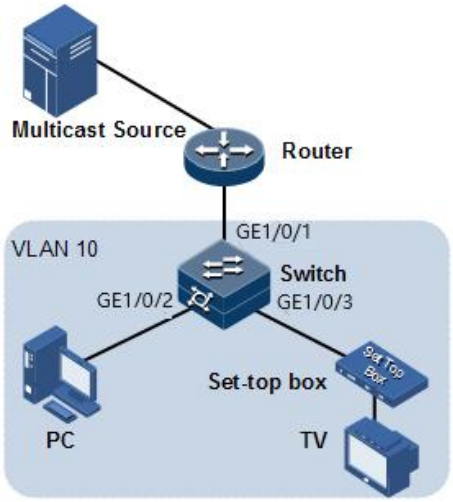
6.3.18 配置 MLD Snooping Proxy 应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 MLD Snooping 功能

在交换机上开启 MLD Proxy 功能，减少主机和组播路由器之间的通信，同时又不影响组播功能实现。

图 6-15 MLD Snooping Proxy 功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 MLD Snooping 功能

```
JX(config)#mld-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#mld-snooping enable
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#mld-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#mld-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#mld-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置开启 MLD Proxy 功能

```
JX(config)#vlan 10
JX(config-vlan-10)#mld-snooping workmode mld-proxy
JX(config-vlan-10)#mld-snooping querier enable
JX(config-vlan-10)#quit
```

检查结果

查看 MLD Snooping 配置信息是否正确。

```
JX#show mld-snooping config
!
mld-snooping start
!
vlan 10
 mld-snooping enable
 mld-snooping workmode mld-proxy
 mld-snooping querier enable
!
interface ge 1/0/1
 mld-snooping enable
!
interface ge 1/0/2
 mld-snooping enable
!
interface ge 1/0/3
 mld-snooping enable
```

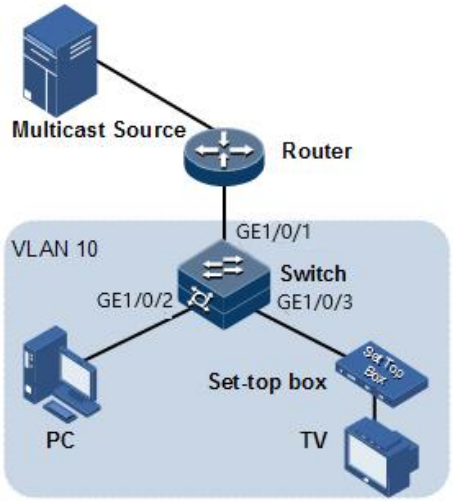
6.3.19 配置 MLD Snooping 策略应用示例

组网需求

如下图所示，交换机接口 Gigaethernet 1/0/1 连接组播路由器，接口 Gigaethernet 1/0/2，Gigaethernet 1/0/3 连接用户，用户在同一个 VLAN 10 中，配置 MLD Snooping 功能

在交换机上开启组播策略功能，接口 Gigaethernet 1/0/2 的用户允许加入 ff1e::1 ~ ff1e::3，接口 Gigaethernet 1/0/3 的用户允许加入 ff1e::4 ~ ff1e::6。

图 6-16 MLD Snooping 组播策略功能组网应用示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 10
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 10
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type access
JX(config-ge-1/0/2)#port default vlan 10
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port link-type access
JX(config-ge-1/0/3)#port default vlan 10
JX(config-ge-1/0/3)#quit
```

步骤 2 配置使能 MLD Snooping 功能

```
JX(config)#mld-snooping start
JX(config)#vlan 10
JX(config-vlan-10)#mld-snooping enable
JX(config-vlan-10)#quit
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#mld-snooping enable
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#mld-snooping enable
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#mld-snooping enable
JX(config-ge-1/0/3)#quit
```

步骤 3 配置 GE1/0/2 用户的 ACL 模板

```
JX(config)#acl-ipv6 3001
JX(configure-acl-ipv6-3001)#rule 1 src-ip any dst-ip ff1e::1/128
JX(configure-acl-ipv6-3001)#rule 1 action permit
JX(configure-acl-ipv6-3001)#rule 2 src-ip any dst-ip ff1e::2/128
JX(configure-acl-ipv6-3001)#rule 2 action permit
JX(configure-acl-ipv6-3001)#rule 3 src-ip any dst-ip ff1e::3/128
JX(configure-acl-ipv6-3001)#rule 3 action permit
JX(configure-acl-ipv6-3001)#quit
```

步骤 4 配置 GE1/0/3 用户的 ACL 模板

```
JX(config)#acl-ipv6 3002
JX(configure-acl-ipv6-3002)#rule 1 src-ip any dst-ip ff1e::4/128
JX(configure-acl-ipv6-3002)#rule 1 action permit
JX(configure-acl-ipv6-3002)#rule 2 src-ip any dst-ip ff1e::5/128
JX(configure-acl-ipv6-3002)#rule 2 action permit
JX(configure-acl-ipv6-3002)#rule 3 src-ip any dst-ip ff1e::6/128
JX(configure-acl-ipv6-3002)#rule 3 action permit
JX(configure-acl-ipv6-3002)#quit
```

步骤 5 配置接口绑定组播策略 ACL 模板

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#mld-snooping group-policy acl-ipv6 3001
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#mld-snooping group-policy acl-ipv6 3002
JX(config-ge-1/0/3)#quit
```

检查结果

查看 MLD Snooping 配置信息是否正确。

```
JX#show mld-snooping config
!
mld-snooping start
!
vlan 10
 mld-snooping enable
!
interface ge 1/0/2
 mld-snooping enable
 mld-snooping group-policy acl-ipv6 3001 version 1-2
!
interface ge 1/0/3
 mld-snooping enable
 mld-snooping group-policy acl-ipv6 3002 version 1-2
```

查看 ACL 模板配置是否正确。

```
JX#show acl config
!
acl-ipv6 3001
 rule 1 src-ip any dst-ip ff1e::1/128
 rule 1 action permit
 rule 2 src-ip any dst-ip ff1e::2/128
 rule 2 action permit
```

```
 rule 3 src-ip any dst-ip ff1e::3/128
 rule 3 action permit
acl-ipv6 3002
 rule 1 src-ip any dst-ip ff1e::4/128
 rule 1 action permit
 rule 2 src-ip any dst-ip ff1e::5/128
 rule 2 action permit
 rule 3 src-ip any dst-ip ff1e::6/128
 rule 3 action permit
```

7 OAM

本章介绍 OAM 特性的基本原理和配置过程，并提供相关的配置案例。

- 简介
- EFM
- 故障转移
- VRRP
- CFM

7.1 简介

以太网最初为局域网设计，由于规模较小，所以 OAM（Operation，Administration and Maintenance，运行、管理和维护）能力较弱，且只有网元级的管理系统。随着以太网技术的不断发展，以太网在电信级网络中的应用也越来越广泛，但电信级网络在链路长度和网络规模上都较局域网大很多，有效管理维护机制的缺乏，已成为以太网技术在电信级网络中应用的严重障碍。

为了在以太网层能确定以太网虚链接的连通性，有效地检测、确认并定位以太网层网络内部的故障，并且可以衡量网络的利用率以及度量网络的性能，从而能根据与用户签订的 SLA（Service Level Agreement，服务等级协议）提供业务，在以太网上实现 OAM 机制已经成为必然的发展趋势。

工作模式

使能 EFM OAM 功能的接口称为 OAM 实体。EFM OAM 支持以下两种工作连接模式：

- 主动模式：连接过程由处于主动模式的 OAM 实体发起；
- 被动模式：处于被动模式的 OAM 实体只能等待对端 OAM 实体的连接请求。如果链路两端的 OAM 实体都处于被动模式，则无法建立 OAM 连接。

OAM 发现

OAM 发现阶段是 OAM 实体发现对端设备的 OAM 实体，并与之建立稳定对话的过程。

本阶段由主动模式的 OAM 实体发起，两端通过交互配置信息 OAM PDU 通报各自的 OAM 配置信息及本地节点支持的 OAM 能力信息，并决定是否同意建立 OAM 连接。如果两端都同意建立 OAM 连接，则 OAM 协议将在链路层开始正常工作。

以太网 OAM 连接建立后，两端的 OAM 实体通过发送 Information OAM PDU 保持连接。若在超时时间内未收到对端 OAM 实体的 Information OAM PDU，则认为连接超时，需要重新建立 OAM 连接。

对端故障通知

当设备发生故障或不可用时将会导致网络中断，因此，OAM PDU 定义了一个标志位（Flag 域）允许 OAM 实体不断发送 Information OAM PDU 给对端，告知此故障信息。

- 链路故障（Link Fault）：对端链路信号丢失，每秒发送 1 次 OAM PDU。
- 致命故障（Dying Gasp）：设备发生导致系统不能恢复的不可预知的故障，不间断发送 OAM PDU。例如电源中断等。
- 严重事件（Critical Event）：设备发生不能确定的紧急事件，不间断发送 OAM PDU。例如温度异常等。

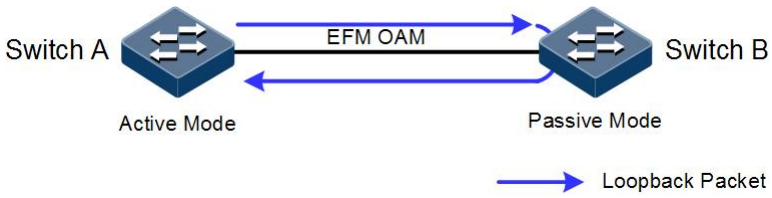
远端环回

远端环回功能可用于定位故障发生的区域，同时借助仪器仪表还可以对链路质量进行测试。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定位故障发生的具体区域，有助于用户排除故障。

OAM 环回只有在以太网 OAM 连接建立完成后才能实现。在连接建立的情况下，主动模式的 OAM 实体发起 OAM 环回命令，对端实体对该命令进行响应。当对端处于环回模式时，除 OAM PDU 报文以外的所有报文都将按原路返回。

如图 7-1 所示，本地处于主动模式的 Switch A 设备将通过返回报文的情况，确定链路状况。

图 7-1 OAM 环回示意图



7.2 EFM

7.2.1 简介

遵循 IEEE 802.3ah 协议的 EFM（Ethernet in the First Mile，第一公里以太网）是一种链路级以太网 OAM 技术，针对两台直连设备之间的链路，提供链路连通性检测功能、

链路故障监控功能、远端故障通知功能等。EFM 主要用于用户接入的网络边缘的以太网链路。

7.2.2 配置准备

场景

在直连设备之间部署 EFM 特性可以有效提高对以太网链路的管理和维护能力，保障网络的稳定运行。

前提

需要连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

7.2.3 缺省配置

设备上 EFM 的缺省配置如下。

功能	缺省值
EFM 工作模式	主模式
报文发送间隔	10×100ms
链路超时时间	5s
EFM 远端环回状态	不响应
误帧事件监控窗口	1s
误帧事件监控阈值	1 个错误帧
误帧周期事件监控窗口	1000ms
误帧周期事件监控阈值	1 个错误帧
链路误帧秒统计事件的监控窗口	100s
链路误帧秒统计事件的监控阈值	1s
误符号周期事件监控窗口	1s
误符号周期事件监控阈值	1s
故障指示功能状态	使能

7.2.4 配置 EFM 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number* Example: JX(config)#interface ge **1/0/1**	进入物理接口配置模式。 interface-type：接口类型 interface-number：接口号
3	JX(config-ge-1/0/1)#**efm max-rate value** Example: JX(config-ge-1/0/1)#**efm max-rate 5**	（可选）最大发送速率限制 EFM 占用的带宽，保证在一定时间间隔内最多只能发送一定数量的 EFMPDU，设置范围为 1 到 10，默认为 10. value：单位时间内发送个数
4	JX(config-ge-1/0/1)#**efm min-rate value** Example: JX(config-ge-1/0/1)#**efm min-rate 5**	（可选）如果本地 EFM 实体在发现超时时间内没有收到对端的 EFMPDU，认为发现连接失败，重启发现过程。设置范围为 1～10，默认为 10 秒。 value：超时时间
5	JX(config-ge-1/0/1)#**efm mode** { **active** | **passive** } JX(config-ge-1/0/1)#**exit** Example: JX(config-ge-1/0/1)#**efm active**	配置 EFM 的工作模式。 配置时至少有一端为主动模式，否则链路检测无法进行。 active：主动模式，接口主动发送 OAM PDU（Protocol Data Unit，协议数据单元），从而发起对端发现或远端环回过程 passive：被动模式，接口被动等待对端发送的 OAM PDU
6	JX(config-ge-1/0/1)#**exit**	进入全局配置模式。
7	JX(config)#**efm** { **enable** | **disable** } Example: JX(config-ge-1/0/1)#**efm enable**	使能接口的 EFM OAM 功能。 enable：使能链路的 EFM OAM 功能 disable：禁用链路的 EFM OAM 功能

7.2.5 配置 EFM 端口环回功能

配置 OAM 远端环回功能

OAM 提供链路层远端环回机制，可用于链路错误定位和性能以及质量测试。当处于链路环回状态时，设备将该链路收到的除了 OAM 报文外的所有报文环回到对端设备。本端设备通过 OAM 远端环回命令发起或者关闭远端环回，对端设备则通过环回配置命令控制是否响应环回命令。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**efm remote-loopback timeout value** Example: JX(config-ge-1/0/1)#**efm remote-loopback timeout 5**	（可选）本地等待响应的时间即为此响应超时时间，如果在此时间内没有收到对方以处于环回状态的响应，设置将失败。设置范围为 1 到 10 秒，默认为 10s value：超时时间
4	JX(config-ge-1/0/1)#**efm remote-loopback** { **supported** | **unsupported** } Example:	配置环回功能支持与否，默认为不支持 supported ：支持 unsupported：不支持
5	JX(config-ge-1/0/1)#**efm min-rate 5**	（可选）如果本地 EFM 实体在发现超时时间内没有收到对端的 EFMPDU，认为发现连接失败，重启发现过程。设置范围为 1～10，默认为 10 秒。 value：超时时间
6	JX(config-ge-1/0/1)#**efm remote-loopback start holdtime** { *hold-time* | **default** } Example: JX(config-ge-1/0/1)#**efm remote-loopback start holdtime 100**	配置环回功能开始，为避免由于用户忘记停止 EFM 远端环回而造成链路长时间无法正常转发业务数据， EFM 远端环回具有超时自动取消功能。holdtime 表示远端环回持续时间。缺省情况下，远端环回的持续时间是 20 分钟，到达此时间，远端环回自动取消。
7	JX(config-ge-1/0/1)#**efm mode remote-loopback stop** Example: JX(config-ge-1/0/1)#**efm mode remote-loopback stop**	配置环回功能结束

7.2.6 配置 EFM 链路故障检测功能

序号	检查项	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number* Example: JX(config)#interface ge **1/0/1**	进入物理接口配置模式。 interface-type：接口类型 interface-number：接口号

序号	检查项	说明
3	JX(config-ge-1/0/1)#**efm critical-event { supported | unsupported }** Example: JX(config-ge-1/0/1)#**efm critical-event supported**	使能端口的 efm 紧急事件监测 supported ： 支持 unsupported：不支持

7.2.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show efm session { all | interface** *interface-type interface-number* **}**	显示两端 EFM 会话信息
2	JX#**show efm status { all | interface** *interface-type interface-number* **}**	显示两端 EFM 配置信息
4	JX#**show efm fault-logs interface** *interface-type interface-number*	显示两端 EFM 错误日志信息
5	JX#**show efm { config | fault-logs | interface | session }**	显示所有使能 EFM 的接口概要信息

7.3 故障转移

7.3.1 简介

故障转移功能提供了一种接口联动方案，可以扩展链路备份的范围，即通过监控上行链路并对下行链路进行同步设置，将上、下行接口加入到一个故障转移组中，使上层设备的故障迅速传达给下层，从而触发主备切换。故障转移功能可避免因上行链路故障无法被下层设备感知而出现的流量丢失。

一旦上行接口全部故障，则下行接口就会被置为 Down 状态，并且只要有一个上行接口恢复后，下行接口就将恢复 Up 状态，从而及时的将上行链路的故障情况通知到下层设备。下行接口故障时不影响上行接口。

7.3.2 配置准备

场景

中间设备上行链路故障时，如无法及时通知下层设备，会导致流量不能切换到备份路径，从而产生流量中断。

故障转移特性将中间设备的上行接口和下行接口加入同一故障转移组，并实时监控上行接口，当上行接口全部故障时，使上层设备的故障迅速传达给下层，保证主链路向备份链路的快速切换，以尽可能减少流量丢失。

前提

无

7.3.3 故障转移功能的缺省配置

设备上故障转移功能的缺省配置如下。

功能	缺省值
故障转移组	无
接口故障处理动作	无
故障转移组 Trap 告警功能	禁止

7.3.4 配置故障转移

说明

故障转移支持物理接口及聚合组接口配置。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**monitor-link group** *group-number*	创建转移组并使能故障转移功能。
3	JX(config-monitorlink-*)#**snmp-trap (enable|disable)**	配置故障转移上报 Trap 功能。
5	JX(config-monitorlink-*)#**add interface** *interface-type interface-number* **role** uplink	配置 uplink
6	JX(config-monitorlink-*)#**add interface** *interface-type interface-number* **role** downlink	配置 downlink

说明

一个故障转移组中可以有多个上行接口，只要有一个上行接口为 Up 状态就不会发生故障转移；只有当全部上行接口都为 Down 的状态时才发生故障转移。

在故障转移节点下，使用 **remove interface** *interface-type interface-number* 命令从故障转移组中删除一个接口。

在物理层接口节点下，使用 **no monitor-link group** *group-number* 命令从故障转移组中删除一个接口。

7.3.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show monitor-link group** *group-number* JX#**show monitor-link group**	查看故障转移组配置和状态信息。

7.3.6 配置故障转移示例

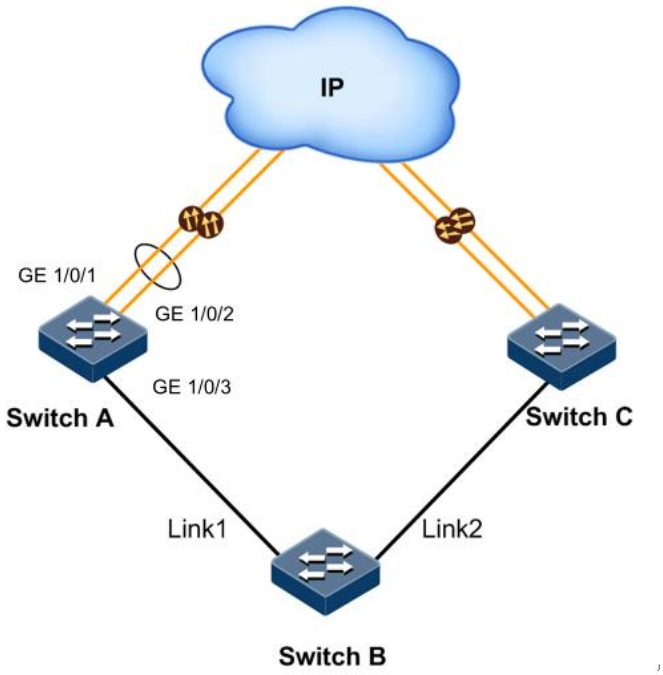
组网需求

如下图所示，为提高网络可靠性，Switch B 通过 Link1 和 Link2 两条链路分别连接到 Switch A 和 Switch C，Link1 为主链路，Link2 为备份链路，只有在 Link1 故障时，才启用 Link2 转发数据。

Switch A 和 Switch C 上行通过链路聚合的方式与上级网络相连，在 Switch A 或 Switch C 上行链路全部故障时，需要及时让 Switch B 感知，从而及时将流量切换到备份链路。

所以需要在 Switch A 和 Switch C 上部署故障转移特性。

图 7-2 故障转移应用组网示意图



配置步骤

配置 Switch A 和 Switch C 的故障转移功能，配置步骤相同，以配置 Switch A 为例。

步骤 1 创建链路聚合组 1，并将上行口 GE 1/0/1 和 GE 1/0/2 加入到链路聚合组中。

```
JX#configure
JX(config)#int eth-trunk 1
JX(config-eth-trunk-1)#add interface ge 1/0/1
JX(config-eth-trunk-1)#add interface ge 1/0/2
```

步骤 2 创建故障转移组 1，将链路聚合组接口加入到故障转移组中。

```
JX(config)#monitor-link group 1
JX(config-monitorlink-1)#add interface eth-trunk 1 role uplink
```

步骤 3 将下行接口 GE 1/0/3 加入到故障转移组中。

```
JX(config-monitorlink-1)#add interface ge 1/0/3 role downlink
```

检查结果

以 Switch A 为例，通过 **show monitor-link group** 查看故障转移组配置是否正确。

```
SwitchA#show monitor-link group 1
Mlink group 1 :
------------------------------------------------------------------------------
-------
 Snmp trap          : enable
 HoldOff time       : 3
```

```
 Uplink-select       : first-up
 Member            Role         State    Status   Linkstate
 ge-1/0/3          downlink      forward   active    up/up
 eth-trunk-1       uplink        forward   active    up/up
--------------------------------------------------------------------------
-------
```

Switch A 上行链路均故障后，再次通过 **show monitor-link group** 查看故障转移组配置可以看到已经发生故障转移。

```
SwitchA#show link-state-tracking group 1
Mlink group 1 :
--------------------------------------------------------------------------
-------
 Snmp trap          : enable
 HoldOff time       : 3
 Uplink-select      : first-up
 Member            Role         State    Status   Linkstate
 ge-1/0/3          downlink      block    active    up/down
 eth-trunk-1       uplink        block    active    up/down
--------------------------------------------------------------------------
-------
```

7.4 VRRP

7.4.1 简介

内部网络中的所有主机都设置一条相同的缺省路由，指向出口网关，实现主机与外部网络的通信。如果网关发生故障，以该网关为缺省路由的主机将无法与外部进行通信。

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是为消除在静态缺省路由环境下，缺省路由设备单点故障引起的网络失效而设计的主备模式协议，有效避免单一链路发生故障引起的网络中断，且无需修改相应的路由协议等配置。

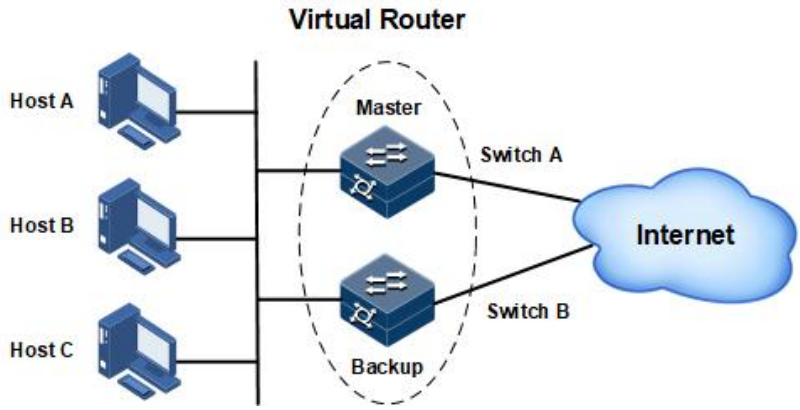
VRRP 备份组

VRRP 协议将局域网内的两台或多台路由设备虚拟成一个设备（包括一个 Master 设备和若干个 Backup 设备），组成一个 VRRP 备份组。VRRP 备份组功能上相当于一台虚拟路由器，对外提供虚拟路由设备的 IP 地址。

- Master 设备：拥有对外 IP 地址的设备如果工作正常，则为 Master 设备，或者通过算法选举产生。Master 设备实现针对虚拟路由设备 IP 地址的各种网络功能。VRRP 协议运行时 Master 设备定时向 Backup 设备发送 VRRP 通告报文，表示其工作正常。
- Backup 设备：不拥有对外 IP 地址或者优先级低的设备，则为 Backup 设备。只接收通告报文，不进行发送。当 Master 设备失效时，从 Backup 设备中重新选举 Master 设备，并接管原先 Master 设备的网络功能。

配置 VRRP 协议时需要为每台路由设备配置备份组号和优先级，使用备份组号将设备进行分组，具有相同备份组号的设备为同一个组。同一组中的设备通过优先级来选举 Master 设备，优先级大的为 Master 设备，如下图所示。

图 7-3 VRRP 原理示意图



在上图中，Switch A 和 Switch B 组成一个虚拟路由设备，此设备拥有自己的 IP 地址。局域网内的主机将虚拟路由设备设置为缺省网关。Switch A 和 Switch B 中优先级最高的设备为 Master 设备，承担网关的功能，另一台设备为 Backup 设备。

VRRP 工作模式

在 VRRP 备份组中，设备具有以下两种工作模式：

- 非抢占模式：只要 Master 设备正常，Backup 设备即使被配置了更高的优先级也不会成为 Master 设备。
- 抢占模式：VRRP 备份组中，设备一旦发现自己的优先级比当前 Master 设备的优先级高，就会对外发送 VRRP 通告报文，导致备份组内设备重新选举 Master，并最终取代原有的 Master 设备。相应地，原来的 Master 设备将会变成 Backup 设备。

VRRP 工作过程

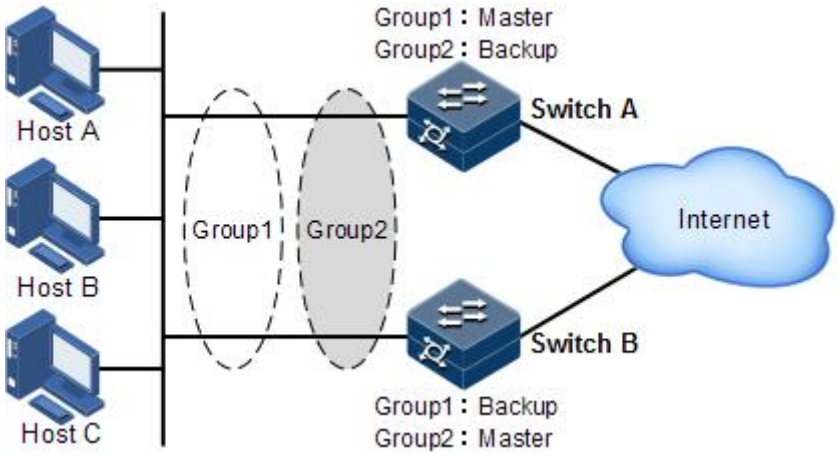
VRRP 的工作过程如下：

1. 设备使能 VRRP 功能后，通过优先级来确定自身在 VRRP 备份组中的角色。优先级高的为 Master，优先级低的为 Backup。Master 定期发送 VRRP 通告报文，通知备份组内的其他设备自身工作正常；Backup 则启动定时器等待通告报文的到来。
2. 抢占模式下，Backup 收到 VRRP 通告报文后，将自身优先级与通告报文中的优先级进行比较。如果小于通告报文中的优先级，则保持 Backup 状态；否则将成为 Master 设备。
3. 非抢占模式下，只要 Master 设备没有出现故障，备份组中的设备状态始终保持不变。
4. 如果 Backup 设备的定时器超时，则认为 Master 设备已经无法正常工作，此时 Backup 设备会认为自己是 Master 设备，并对外发送 VRRP 通告报文，进行新一轮 Master 设备的选举。新选举出来的 Master 设备将接管原先 Master 设备的网络功能，承担报文转发功能。

负载分担

VRRP 负载分担是指建立两个或者多个 VRRP 备份组，多台设备同时承担业务。允许一台设备为多个备份组作备份，在不同备份组中具有不同的优先级。通过多个虚拟设备可以实现负载分担。各个备份组的 Master 可以不同，如下图所示。

图 7-4 VRRP 负载分担原理示意图



其中：

- Switch A 为 VRRP 备份组 1 的 Master 设备，同时为备份组 2 的 Backup 设备。
- Switch B 为 VRRP 备份组 2 的 Master 设备，同时为备份组 1 的 Backup 设备。

网络内部分主机使用备份组 1 作为网关，例如 Host A 和 Host B，部分主机使用备份组 2 作为网关，例如 Host C。这样，既达到相互备份的目的，又可以分担网络流量。

7.4.2 配置准备

场景

在网络环境中，通常会为同局域网内的所有主机配置一条指向出口网关的缺省路由，实现局域网内主机与外部网络之间的通信。如果该网关发生故障，则局域网内主机与外部网络的通信就会中断。

VRRP 技术将多台路由器组合到一起形成备份组，用户通过为备份组配置虚拟 IP 地址，使用时只需要将局域网主机的缺省网关配置为备份组的虚拟 IP 地址，即可实现局域网内主机与外部网络之间的通信。

VRRP 功能的部署可以提高网络的可靠性，有效避免因为单一链路中断而造成的网络中断的问题，也无需因为链路中断而更改路由配置。

前提

无

7.4.3 VRRP 的缺省配置

设备上 VRRP 的缺省配置如下。

功能	缺省值
VRRP 功能状态	使能
VRRP 的 Trap 功能状态	去使能
接口下 VRRP 组	无
VRRP 备份组描述	无
VRRP 备份组功能状态	去使能
设备优先级	100
IP 拥有者优先级	255
VRRP 工作模式	抢占模式
VRRP 组的抢占延时	0s
VRRP 组的报文发送间隔	1s

7.4.4 配置 VRRP 备份组

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	JX(config-vlan*)#**vrrp** *group-id* **virtual-ip** *ipv4-address*	配置 VRRP 备份组的虚 IPv4 地址
4	JX(config-vlan*)#**vrrp** group-id **advertise-interval** { *interval* | **default** }	（可选）配置协议包发送间隔 group-id：VRRP 实例号。 interval,：协议包发送间隔时间，单位为秒，取值范围为 1～4000，默认值为 1 default：默然协议包发送间隔时间。
5	JX(config-vlan*)#**vrrp** *group-id* **check-ttl** { **enable** | **disable** }	可选）配置检测协议包 ttl 使能 group-id：VRRP 实例号 enable:使能 disable：去使能 默认使能

步骤	配置	说明
6	JX(config-vlan*)#**vrrp** *group-id* **priority** { value | **default** }	（可选）VRRP 实例优先级 group-id：VRRP 实例号 (value|default)：优先级大小，默认为 100.
7	JX(config-vlan*)#**vrrp** *group-id* **bfd** *bfd-session* **increased {** *increased-value* **| default }** JX(config-vlan*)#**vrrp** *group-id* **bfd** *bfd-session* **reduced {** *reduced-value* **| default }** JX(config-vlan*)#**vrrp** *group-id* **bfd** *bfd-session*	（可选）绑定 bfd group-id：VRRP 实例号 bfd-id:bfd 实例号 （可选）increased：提高优先级 （可选）increased：降低优先级 （可选）value|default：配置当 bfd 状态 down 时，当前 vrrp 实例需减少的优先级大小，默认为 10
8	JX(config-vlan*)#**vrrp** *group-id* **track interface vlan** *vlan-id*	（可选）配置绑定关联 vlan 接口 group-id：VRRP 实例号 vlan-id：绑定的 vlan 索引
9	JX(config-vlan*)#**vrrp** *group-id* **track admin-vrrp interface vlan** *vlan-id vrrp-id* JX(config-vlan*)#**vrrp** *group-id* **track admin-vrrp interface** { **10ge** | **ge** | **eth** } *interface-number* **vrid** *vrid-id*	（可选）配置绑定关联管理 vrrp 组 group-id：VRRP 实例号 vlan-id：绑定的 vlan 索引 vrrp-id：管理 vrrp 实例号
10	JX(config-vlan*)#**vrrp** *group-id* **send-packet-mode** { **v2** | **v3** | **v2v3** }	（可选）配置发送的 vrrp 报文版本 group-id：VRRP 实例号 v2：发送 v2 报文 v3：发送 v3 报文 v2v3:同时发送 v2 和 v3 报文
11	JX(config-vlan*)#**vrrp** *group-id* **authentication-mode** { **simple** | **md5** } { **cipher** | **plain** } **key**	（可选）vrrp 认证，只对 v2 实例生效 group-id：VRRP 实例号 simple：简单字符认证 md5：md5 认证 cipher：密文显示 plain: 明文显示 key：认证字符
12	JX(config-vlan*)#**vrrp** *group-id* **holding-multiplier** [**holding-multiplier-value**]	（可选）vrrp backup 超时倍数 group-id：VRRP 实例号 holding-multiplier-value：超时倍数（3-10），默认为 3

步骤	配置	说明
13	JX(config-vlan*)#**vrrp** *group-id* **role admin**	（可选）配置 vrrp 角色管理 group-id：VRRP 实例号

7.4.5 配置 VRRP6 备份组

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	JX(config-vlan*)#**ipv6 enable**	开启 IPv6 功能。
4	JX(config-vlan*)#**vrrp-ipv6** *group-id* **associate-address** *ipv6-address* **[link-local]**	配置 VRRP 备份组的虚 IPv6 地址 第一个虚 IP 地址必须先配置带 link-local 地址才能配置其他虚 ip（虚拟网关地址），linklocal 地址不可作为虚拟网关。
5	JX(config-vlan*)#**vrrp-ipv6** *group-id* **advertise-interval** { *interval* | **default** }	（可选）配置协议包发送间隔 group-id：VRRP6 实例号。 (interval|default)：协议包发送间隔时间，单位为秒，默认值为 100
6	JX(config-vlan*)#**vrrp-ipv6** *group-id* **check-ttl** { **enable** | **disable** }	（可选）配置检测协议包 ttl 使能 group-id：VRRP6 实例号 enable:使能 disable：去使能 默认使能
7	JX(config-vlan*)#**vrrp-ipv6** *group-id* **priority** { *value* | **default** }	（可选）VRRP6 实例优先级 group-id：VRRP 实例号 (value|default)：优先级大小，默认为 100.
8	JX(config-vlan*)#**vrrp-ipv6** *group-id* **track bfd** *bfd-id* [{ **increased** | **reduced** } { *value* | **default** }]	（可选）绑定 bfd group-id：VRRP6 实例号 bfd-id:bfd 实例号 （可选）increased：提高优先级 （可选）increased：降低优先级 （可选）value|default：配置当 bfd 状态 down 时，当前 vrrp 实例需减少的优先级大小，默认为 10

步骤	配置	说明
9	JX(config-vlan*)#**vrrp-ipv6** *group-id* **track interface vlan** *vlan-id*	（可选）配置绑定关联 vlan 接口 group-id：VRRP6 实例号 vlan-id：绑定的 vlan 索引
10	JX(config-vlan*)#**vrrp-ipv6** *group-id* **track admin-vrrp interface vlan** *vlan-id* **vrid** *vrrp-id*	（可选）配置绑定关联管理 vrrp 组 group-id：VRRP6 实例号 vlan-id：绑定的 vlan 索引 vrrp-id：管理 vrrp 实例号
11	JX(config-vlan*)#**vrrp-ipv6** *group-id* **holding-multiplier** { *holding-multiplier-value* | **default** }	（可选）vrrp6 backup 超时倍数 group-id：VRRP6 实例号 holding-multiplier-value：超时倍数（3-10），默认为 3
12	JX(config-vlan*)#**vrrp-ipv6** *group-id* **role admin**	（可选）配置 vrrp 6 角色管理 group-id：VRRP 实例号

7.4.6 配置 VRRP 的 Trap 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**vrrp snmp-trap** { **enable** | **disable** }	使能/去使能 VRRP 的 Trap 功能。

7.4.7 配置 VRRP 监视接口

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	JX(config-vlan*)#**vrrp** *group-id* **track** { *interface-type interface-number* | **vlan** *vlan-id* } [{ **increased** | **reduced** } { **value** | **default** }]	配置 VRRP 监视接口功能。

reduced *priority*：当被监视接口从 UP 状态变为 DOWN 状态时，优先级减少的数值，整数形式，取值范围是 1～255，不配置该参数，设备在备份组中的优先级在原有基础上降低 10，减少后的优先级范围是 1～254

当被监视接口从 DOWN 状态变为 UP 状态时，优先级恢复原来的数值，建议在 Master 设备进行配置。

7.4.8 配置 BFD for VRRP

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	JX(config-vlan*)#**vrrp** *group-id* **track bfd** *bfd-id* [{ **increased** | **reduced** } { **value** | **default** }]	配置 VRRP 备份组对 BFD 会话进行监测，以达到快速切换的目的。

increased *priority*：配置当被监视的 BFD 会话状态变为 DOWN 时，优先级增加的数值，整数形式，取值范围是 1～255，增加后的优先级范围是 1～254。如果从 DOWN 状态变为 UP 状态，则优先级恢复原来的数值。建议在 Backup 设备上进行配置。

reduced *priority*：配置当被监视的 BFD 会话状态变为 DOWN 时，优先级降低的数值，整数形式，取值范围是 1～255，减少后的优先级范围是 1～254。如果从 DOWN 状态变为 UP 状态，则优先级恢复原来的数值。建议在 Master 设备上进行配置。

7.4.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show vrrp session { role { admin | member | normal } }**	显示 VRRP 基本状态信息。
2	JX#**show vrrp admin-vrrp**	显示管理 VRRP 信息
3	JX#**show vrrp statistics**	显示 VRRP 统计信息

序号	检查项	说明
4	JX#**show vrrp interface vlan** *vlan-id* JX#**show vrrp interface { 10ge | ge | eth }** *interface-number*	显示接口上的 vrrp 信息。
5	JX#**show vrrp associate interface vlan** *vlan-id* [**vrid** *group-id*] JX#**show vrrp associate interface { 10ge | ge | eth }** *interface-number* [**vrid** *group-id*] JX#**show vrrp associate interface**	显示接口上指定 group id 的 VRRP 信息
6	JX#**show vrrp binding admin-vrrp interface vlan** *vlan-id* **vrid** *group-id* JX#**show vrrp binding admin-vrrp interface interface { 10ge | ge | eth }** *interface-number* **vrid** *group-id*	显示 VRRP 管理组绑定信息

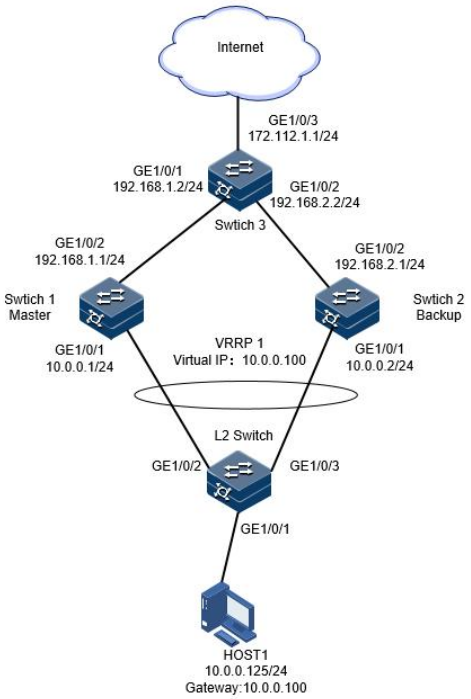
7.4.10 配置 VRRP 主备示例

组网需求

如图 7-5 所示，Host1 通过 Switch 双归属到 Switch1 和 Switch2。为保证用户的各种业务在网络传输中不中断，需在 Switch1 和 Switch2 上配置 VRRP 主备备份功能。

正常情况下，主机以 Switch1 为默认网关接入 Internet，当 Switch1 故障时，Switch2 接替 Switch1 作为网关继续进行工作，实现网关的冗余备份。

图 7-5 配置 VRRP 主备组网图



配置步骤

步骤 1 配置 L2 Swtich 二层转发

```
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/2
L2switch(config-ge-1/0/2)#port hybrid pvid 100
L2switch(config-ge-1/0/2)#port hybrid vlan 100 untagged
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/3
L2switch(config-ge-1/0/3)#port hybrid pvid 100
L2switch(config-ge-1/0/3)#port hybrid vlan 100 untagged
```

步骤 2 配置 Switch 1

```
switch1(config)#vlan 100
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#ip address 10.0.0.1/24
switch1(config)#vlan 300
switch1(config)#interface vlan 300
switch1(config-vlanif-300)#ip address 192.168.1.1/24
switch1 (config)#interface ge 1/0/1
switch1(config-ge-1/0/1)#port hybrid pvid 100
switch1(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch1 (config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#port hybrid pvid 300
switch1(config-ge-1/0/2)#port hybrid vlan 300 untagged
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
switch1(config-vlanif-100)#vrrp 1 priority 120
```

步骤 3 配置 Switch 2

```
switch2(config)#vlan 100
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#ip address 10.0.0.1/24
switch2(config)#vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)#ip address 192.168.2.1/24
switch2(config)#interface ge 1/0/1
switch2(config-ge-1/0/1)#port hybrid pvid 100
switch2(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch2(config)#interface ge 1/0/2
switch2(config-ge-1/0/2)#port hybrid pvid 500
switch2(config-ge-1/0/2)#port hybrid vlan 500 untagged
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
```

检查结果

```
switch1#show vrrp session
  Interface             VRID Role   Version VR-State Pri IP-Count State
Auth-Mode   Auth-Key
------------------------------------------------------------------------
--------------------------------
  vlan-100               1    normal 2      Master   120 1       Active
none       N/A
```

```
switch2#show vrrp session
  Interface             VRID Role   Version VR-State Pri IP-Count State
Auth-Mode   Auth-Key
-------------------------------------------------------------------------
---------------------------------
  vlan-100               1    normal 2      Backup   100 1       Active
none       N/A
-------------------------------------------------------------------------
---------------------------------
```

7.5 CFM

7.5.1 简介

CFM 是一种网络级以太网 OAM 技术，针对网络实现端到端的连通性故障检测、故障通告、故障判定和故障定位功能。用于对 EVC（Ethernet Virtual Connection，以太网虚连接）进行主动的故障诊断，并通过使用故障管理功能有效降低网络维护成本，提高以太网的可维护性。

交换机设备遵循 IEEE 802.1ag 的 CFM（Connectivity Fault Management，连通错误管理）协议和 ITU-T 的 Y.1731 协议。

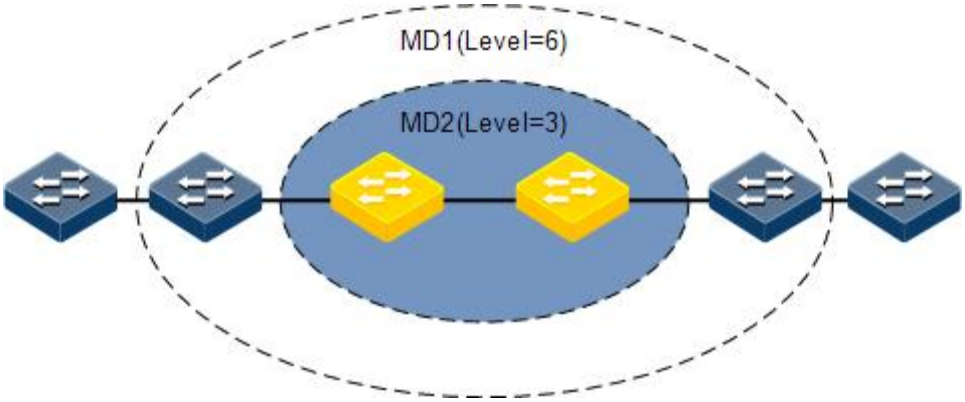
CFM 由如下组件组成：

- MD

维护域 MD（Maintenance Domain，又称 MEG，Maintenance Entity Group，维护实体组）是一个运行 CFM 功能的网络，它确定了进行 OAM 管理的网络范围。维护域具有级别属性，共分为 8 级（0～7），数字越大表示维护域级别越高，对应维护域的范围越大。低级别 MD 的协议报文进入高级别的 MD 后被丢弃，（如果高级别 MD 中不存在 MEP，而只有 MIP，则报文能够通过。）高级别 MD 的协议报文可以穿越低级别的 MD。在同一 VLAN 范围内，不同的维护域之间可以相邻、嵌套，但不能交叉。

如下图所示，MD2 包含在 MD1 中，MD1 的协议报文需要穿越 MD2。因此，将 MD1 的级别配置为 6，MD2 的级别配置为 3，这样 MD1 内的协议报文就可以穿越 MD2 实现整个 MD1 的连通性故障管理，而 MD2 的协议报文不会扩散到 MD1 中。MD2 为服务器层，MD1 为客户层。

图 7-6 不同级别 MD 网络示意图



- MA

MA（Maintenance Association，维护联盟）是 MD 的一部分，一个 MD 可划分为一个或多个 MA。MA 以“MD 名称＋MA 名称”来标识。

MA 可以服务于指定的 VLAN，也可以不服务于任何 VLAN，分别称为带 VLAN 属性和不带 VLAN 属性的 MA。

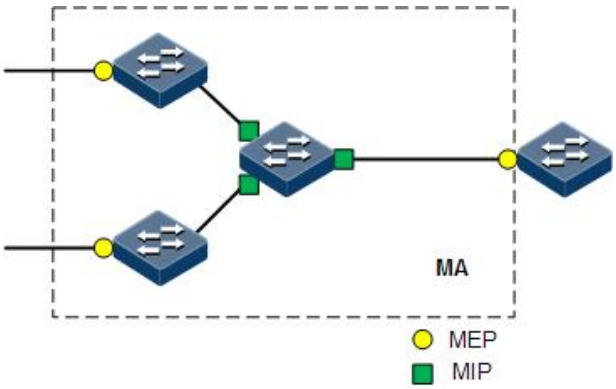
- MEP

如下图所示，MEP（Maintenance association End Point，维护端点）确定了 MA 的边界，以“MEP ID”来标识。MEP 具有方向性，分为内向 MEP 和外向 MEP 两种：

内向 MEP 通过除其所在的接口以外的所有接口向外发送 CFM 协议报文，即在其所属 MA 所服务的 VLAN 中进行广播。

外向 MEP 则直接通过其所在的接口向外发送 CFM 协议报文。

图 7-7 不同级别 MD 网络示意图



- MIP

如上图所示，MIP（Maintenance association Intermediate Point，维护中间点）位于 MA 的内部，不能主动发出 CFM 协议报文，但可以处理和响应 CFM 协议报文。MIP 由设备自动创建，可以配合 MEP 完成类似于 ping 和 tracert 的功能。

- MP

MEP 和 MIP 统称为维护节点 MP（Maintenance Point）。

CFM 能够提供以下 OAM 功能：

- 故障检测功能

故障检测功能是指使用 CC（Continuity Check，连续性检测）协议来检测一个以太网虚连接的连通性，确定 MP 之间的连接状态。该功能通过 MEP 周期性地发送 CCM（Continuity Check Message，连续性检测报文）实现，同一服务实例内其他 MEP 接收该报文，由此确定 RMEP 的状态。如果设备故障或者链路中间配置错误，会导致 MEP 无法正常接收和处理 RMEP 发送的 CCM。如果 MEP 在 3.5 个 CCM 间隔周期内未收到远端的 CCM 报文，则认为链路存在故障，会根据告警优先级配置发送故障告警。

- 故障确认功能

故障确认功能利用 LB（LoopBack，环回功能），通过源 MEP 发送 LBM 和目的 MP 回应 LBR 以确定两个 MP 之间的连通性。源 MEP 发送 LBM 给要进行故障确认的 MP，当该 MP 收到 LBM 报文后，发送一个 LBR 给源 MEP，如果源 MEP 接收到 LBR，则确认路径是连通的，如果源 MEP 没有接收到 LBR，则确认存在连通性故障。

- 故障定位功能

故障定位功能利用 LT（LinkTrace，链路跟踪），通过源 MEP 发送 LTM 给目的 MP，LTM 传输路径上的每个 MP 设备都会回应 LTR 给源 MEP，通过记录有效的 LTR 和 LTM 定位故障点。

Y.1731 是由 ITU-T 标准组织提出的 OAM 协议，它不仅包含 IEEE802.1ag 所规定的内容，而且又增加了更多的 OAM 消息组合，能够提供以下 OAM 功能：

- 告警抑制功能

告警抑制功能用来减少 MEP 故障告警的数量。如果 MEP 在 3.5 个 CCM 报文发送周期内未收到远端 MEP 发来的 CCM 报文，便立刻开始周期性地发送 AIS（Alarm Indication Signal，告警指示信号）报文，该报文的发送方向与 CCM 报文相反。其它 MEP 在收到 AIS 报文后，会抑制本端的故障告警，并继续发送 AIS 报文。此后，如果 MEP 收到了 CCM 报文，便停止发送 AIS 报文并恢复故障告警。AIS 报文是组播报文。

- 单向丢包测试功能

单向丢包测试（Loss Measurement，LM）功能用来检测 MEP 之间的单向丢包情况，其实现方式是：由源 MEP 发送 LMM（Loss Measurement Message，丢包测量报文）报文给目标 MEP，目标 MEP 收到该报文后，会发送 LMR（Loss Measurement Reply，丢包测量应答）报文给源 MEP，源 MEP 则根据两个连续的 LMR 报文来计算源 MEP 和目标 MEP 间的丢包数，即源 MEP 从收到第二个 LMR 报文开始，根据本 LMR 报文和前一个 LMR 报文的统计计数来计算源 MEP 和目标 MEP 间的丢包数。LMM 报文和 LMR 报文都是单播报文。

- 帧时延测试功能

帧时延测试（Delay Measurement，DM）功能用来检测 MEP 之间报文传输的时延情况，分为单向时延测试、双向时延测试两种，目前仅支持双向时延测试。双向时延测试功能的实现方式是：源 MEP 发送 DMM（Delay Measurement Message，时延测量报文）报文给目标 MEP，该报文中携带有其发送时间。目标 MEP 收到该报文后记录其接收时间，然后再发送 DMR（Delay Measurement Reply，时延测量应答）报文给源 MEP，

该报文中携带有 DMM 报文的发送和接收时间，以及 DMR 报文的发送时间。源 MEP 收到 DMR 报文后记录其接收时间，并据此计算出链路传输的时延和抖动。

总之，CFM 实现了在端到端服务层面的 OAM 技术，降低了服务提供商的运行维护成本，在一定程度上可以提高服务提供商的竞争优势。

7.5.2 配置准备

场景

为拓展以太网技术在电信级网络中的应用，以太网需要达到与电信级传送网相同的服务水平。CFM 通过为电信级以太网提供全面的 OAM 工具解决了此问题。

前提

在配置 CFM 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。
- 将接口加入 VLAN。

7.5.3 缺省配置

设备上 CFM 的缺省配置如下。

功能	缺省值
CFM 全局功能状态	禁用
CCM 报文发送时间间隔	1s
MEP 发送 CCM 报文	禁用
CFM OAM 报文优先级	0

7.5.4 配置 CFM 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cfm start**	全局使能 CFM 功能。

步骤	配置	说明
3	JX(config)#**cfm md** *md-name* **level** *level* **format** { **dns** *dns-format-string* | **mac** *mac-format-string* | **string** string | **none** } JX(config)#**cfm md** *md-name* [**level** *level*]	创建 MD，并进入 MD 视图。指定了 MD 的名称，指定发送 CCM 报文中使用的 MD 名称的格式和内容，维护域名称和发送报文中使用的 MD 名称内容必须全局唯一，否则将导致维护域配置失败。
4	JX(config-cfm-md-*-*ma*-*)#**mip create-type** { **default** | **explicit** | **none** }	配置当前 MA 的 MIP 生成规则。 default：如果端口不存在更高级别的 MEP，并且不存在更低级别的 MIP，则可以在该端口上创建 MIP。在本类型下，接口上没有配置 MEP 也可创建 MIP。 explicit：如果端口存在更低级的 MEP 但不存在更高级别的 MEP，而且不存在更低级别的 MIP，则可以创建 MIP。在本类型下，接口上只有已配置了更低级别的 MEP 才可能创建 MIP。 none：如果端口的 MIP 的生成规则为 none 类型，即不自动创建 MIP。
5	JX(config-cfm-md-*)#**ma** *ma-name* **format** { **string** | **icc** } *format-string*	在 MD 内创建 MA，并进入 MA 视图。指定了 MA 的名称以及指定发送 CCM 报文中填充的 MA 名称的格式和内容。同一 MD 内，MA 的名称不能重复。（当 MD format 为 none，MA format 为 icc 时，该模式为 Y1731 模式。）
6	JX(config-cfm-md-*-*ma*-*)#**map vlan** *vlan-id*	配置当前 MA 关联的 VLAN。
7	JX(config-cfm-md-*-*ma*-*)#**mep mep-id** *mep-id* **interface** *interface-type interface-number* { **inward** | **outward** }	在 MA 内创建 MEP。 在同一个 MA 内，对创建 MEP 的数量和类型要求如下： inward 型普通 MEP 和 outward 型普通 MEP 不能同时存在。 只能创建 1 个 outward 接口型 MEP，可以创建多个 inward 接口型 MEP，但是同一个接口上只能创建 1 个 inward 接口型 MEP。

7.5.5 配置故障检测功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cfm md** *md-name*	进入 MD 视图。
3	JX(config-cfm-md-*)#**ma** *ma-name*	进入 MA 视图。
4	JX(config-cfm-md-**ma*-*)#**ccm interval** { **3.3ms** | **10ms** | **100ms** | **1s** | **10s** | **1min** | **10min** | **default** }	配置当前 MA 内 MEP 发送 CCM 消息的时间间隔。 部署 1s 以下的发送 CCM 消息的时间间隔，需要交换芯片支持 CFM。
5	JX(config-cfm-md-**ma*-*)#**ccm send** [**mep-id** *mep-id*] **enable**	使能 MEP 发送 CCM 报文。
6	JX(config-cfm-md-**ma*-*)#**rmep mep-id** *mep-id* **mac** *mac-address*	配置静态远端 MEP。配合 CCM 报文检测功能使用。
7	JX(config-cfm-md-**ma*-*)#**ccm send** [**mep-id** *mep-id*] **priority** { priority | **default** }	配置 MA 内 MEP 发送 CCM 报文的优先级。

7.5.6 配置故障确认功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cfm md** *md-name*	进入 MD 视图。
3	JX(config-cfm-md-*)#**ma** *ma-name*	进入 MA 视图。

步骤	配置	说明
4	JX(config-cfm-md-*-*ma-*)#**ping mep-id** *mep-id* **rmep-id** *mep-id* [**count** *count* | **tlv-type** { **null** | **null-crc** | **prbs** | **prbs-crc** } | **tlv-len** *len* | **priority** *priority*]* JX(config-cfm-md-*-*ma-*)#**ping mep-id** *mep-id* **mac** *mac-address* [**count** *count* | **tlv-type** { **null** | **null-crc** | **prbs** | **prbs-crc** } | **tlv-len** *len* | **priority** *priority*]* JX(config-cfm-md-*-*ma-*)#**ping mep-id** *mep-id* **mac multicast** [**count** *count* | **tlv-type** { **null** | **null-crc** | **prbs** | **prbs-crc** } | **tlv-len** *len* | **priority** *priority*]*	执行二层 ping 功能，用于故障确认。

7.5.7 配置故障定位功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cfm md** *md-name*	进入 MD 视图。
3	JX(config-cfm-md-*)#**ma** *ma-name*	进入 MA 视图。
4	JX(config-cfm-md-*-*ma-*)#**trace mep-id** *mep-id* **mac** *mac-address* [**ttl** *ttl* | **fdb** *<0-1>*]* JX(config-cfm-md-*-*ma-*)# **trace mep-id** *mep-id* **rmep-id** *mep-id* [**ttl** *ttl* | **fdb** *<0-1>*]*	执行二层 Traceroute 功能，用于故障定位。

7.5.8 配置告警抑制功能（仅在 Y1731 模式下可配置）

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cfm md** *md-name*	进入 MD 视图。
3	JX(config-cfm-md-*)#**ma** *ma-name*	进入 MA 视图。

步骤	配置	说明
4	JX(config-cfm-md-*-*ma-*)#**ais [mep** *mep-id* **] interval { 1s | 1min | default }**	配置当前 MA 内 MEP 向高级别 MA 内 MEP 发送 AIS 报文的时间间隔。
5	JX(config-cfm-md-*-*ma-*)#**ais [mep** *mep-id* **] md-level {** *level* **| defalut }**	配置当前 MA 内 MEP 发送 AIS 报文的级别。
6	JX(config-cfm-md-*-*ma-*)#**ais [mep** *mep-id* **] priority {** *priority* **| defalut }**	配置当前 MA 内 MEP 发送 AIS 报文的优先级。
7	JX(config-cfm-md-*-*ma-*)#**ais [mep** *mep-id* **] enable**	使能 MEP 发送 AIS 报文。

7.5.9 配置单向丢包测试功能（仅在 Y1731 模式下可配置）

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cfm md** *md-name*	进入 MD 视图。
3	JX(config-cfm-md-*)#**ma** *ma-name*	进入 MA 视图。
4	JX(config-cfm-md-*-*ma-*)#**loss-measure mep-id** *mep-id* **rmep-id** *mep-id* **[interval { 100ms | 1s } | priority** *priority* **| count** *<1-100>* **]*** JX(config-cfm-md-*-*ma-*)#**loss-measure mep-id** *mep-id* **mac** *mac-address* **[interval { 100ms | 1s } | priority** *priority* **| count** *<1-100>* **]***	执行单向丢包测试功能，用于检测 MEP 之间的单向丢包情况。

7.5.10 配置双向时延测试功能（仅在 Y1731 模式下可配置）

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cfm md** *md-name*	进入 MD 视图。
3	JX(config-cfm-md-*)#**ma** *ma-name*	进入 MA 视图。

步骤	配置	说明
4	JX(config-cfm-md-*-*ma-*)#**delay-measure mep-id** *mep-id* **rmep-id** *mep-id* [**interval** { **100ms** | **1s** } | **priority** *priority* | **frame-len** *len* | **count** *count*]* JX(config-cfm-md-*-*ma-*)#**delay-measure mep-id** *mep-id* **mac** *mac-address* [**interval** { **100ms** | **1s** } | **priority** *priority* | **frame-len** *len* | **count** *count*]*	执行双向时延测试功能，用于检测 MEP 之间报文传输的时延情况。

7.5.11 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show cfm config**	查看 CFM 配置信息。
2	JX#**show cfm md**	查看 CFM MD 信息。
3	JX#**show cfm ma**	查看 CFM MA 信息。
4	JX#**show cfm mep**	查看 CFM MEP 信息。
5	JX#**show cfm rmep**	查看 CFM 远端 MEP 信息。
6	JX#**show cfm mip**	查看 CFM MIP 信息。

7.5.12 配置 CFM 示例

组网需求

如图 4-10 所示。

由五台设备组成的网络被划分为 MD_A 和 MD_B 两个 MD，其级别分别为 5 和 3，各设备的所有端口都属于 VLAN 100，且各 MD 中的 MA 均服务于该 VLAN，并假定 Device A～Device E 的 MAC 地址依次为 00:03:56:00:00:01、00:03:56:00:00:02、00:03:56:00:00:03、00:03:56:00:00:04 和 00:03:56:00:00:05。

MD_A 的边界端口为 Device A 的 GE1/0/1、Device D 的 GE1/0/3 和 Device E 的 GE1/0/4，这些端口上都是内向 MEP；MD_B 的边界端口为 Device B 的 GE1/0/3 和 Device D 的 GE1/0/1，这些端口都是外向 MEP。

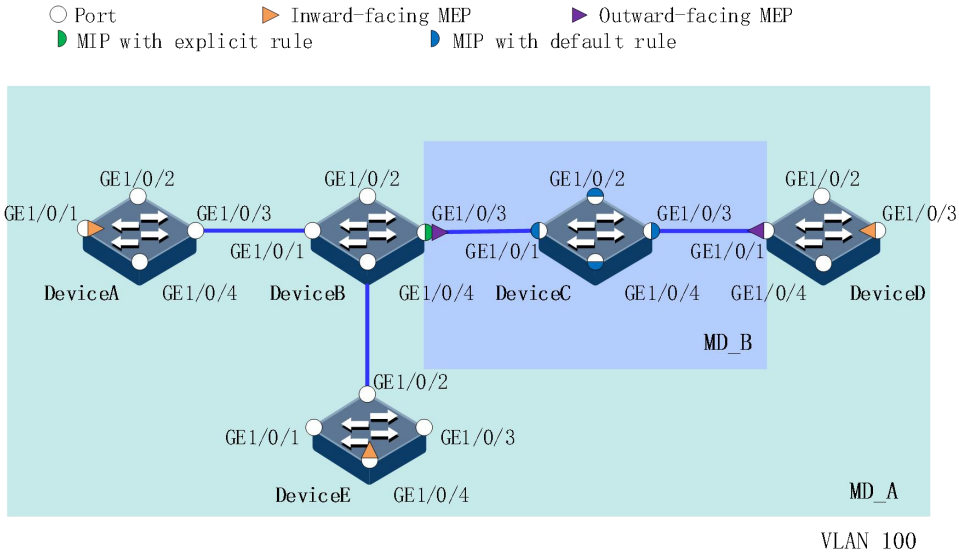
要求将 MD_A 的 MIP 规划在 Device B 上，并只在端口上有低级别 MEP 时配置。根据此规划，由于 Device B 的 GE1/0/3 上配置有 MD_B 的 MEP，因此在 Device B 上采用 Explicit 规则来创建 MD_A 的 MIP，其他 Device 上采用 None 规则。

要求将 MD_B 的 MIP 规划在 Device C 上，并在其所有端口上配置。根据此规划，在 Device C 上配置 MD_B 的 MIP，且其创建规则为 Default 规则，其他 Device 上采用 None 规则。

要求通过使用连续性检测功能来检测 MD_A 和 MD_B 中各 MEP 之间的连通状态，当检测到链路故障时，使用环回功能进行故障定位，并通过告警抑制功能和以太网告警抑制功能来减少故障告警的数量。

要求在获取到整个组网的状态后，分别使用链路跟踪功能、单向丢包测试功能、双向时延测试功能进行各种链路故障检测。

图 7-8 CFM 典型配置组网图



配置步骤

步骤 1 配置 VLAN 和端口。

请按照上图在各设备上分别创建 VLAN 100，并配置端口 GE1/0/1～GE1/0/4 都属于 VLAN 100。

步骤 2 开启 CFM 基本功能。

```
DeviceA#configure
DeviceA(config)#cfm start
DeviceA(config)#cfm md MD_A level 5 format none
DeviceA(config-cfm-md-MD_A)#mip create-type none
DeviceA(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceA(config-cfm-md-MD_A-ma-1)#map vlan 100
DeviceA(config-cfm-md-MD_A-ma-1)#mep mep-id 1001 interface ge 1/0/1
inward
DeviceA(config-cfm-md-MD_A-ma-1)#end
DeviceB#configure
DeviceB(config)#cfm start
DeviceB(config)#cfm md MD_A level 5 format none
DeviceB(config-cfm-md-MD_A)#mip create-type explicit
```

```
DeviceB(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceB(config-cfm-md-MD_A-ma-1)#map vlan 100
DeviceB(config-cfm-md-MD_A-ma-1)#end
DeviceB#configure
DeviceB(config)#cfm md MD_B level 3 format none
DeviceB(config-cfm-md-MD_B)#ma 2 format icc 2
DeviceB(config-cfm-md-MD_B-ma-2)#map vlan 100
DeviceB(config-cfm-md-MD_B-ma-2)#mep mep-id 2001 interface ge 1/0/3
outward
DeviceB(config-cfm-md-MD_B-ma-2)#end

DeviceC#configure
DeviceC(config)#cfm start
DeviceC(config)#cfm md MD_B level 3 format none
DeviceC(config-cfm-md-MD_B)#ma 2 format icc 2
DeviceC(config-cfm-md-MD_B-ma-2)#map vlan 100
DeviceC(config-cfm-md-MD_B-ma-2)#end

DeviceD#configure
DeviceD(config)#cfm start
DeviceD(config)#cfm md MD_A level 5 format none
DeviceD(config-cfm-md-MD_A)#mip create-type none
DeviceD(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceD(config-cfm-md-MD_A-ma-1)#map vlan 100
DeviceD(config-cfm-md-MD_A-ma-1)#mep mep-id 4002 interface ge 1/0/3
inward
DeviceD(config-cfm-md-MD_A-ma-1)#end
DeviceD#configure
DeviceD(config)#cfm md MD_B level 3 format none
DeviceD(config-cfm-md-MD_B)#mip create-type none
DeviceD(config-cfm-md-MD_B)#ma 2 format icc 2
DeviceD(config-cfm-md-MD_B-ma-2)#map vlan 100
DeviceD(config-cfm-md-MD_B-ma-2)#mep mep-id 4001 interface ge 1/0/1
outward
DeviceD(config-cfm-md-MD_B-ma-2)#end

DeviceE#configure
DeviceE(config)#cfm start
DeviceE(config)#cfm md MD_A level 5 format none
DeviceE(config-cfm-md-MD_A)#mip create-type none
DeviceE(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceE(config-cfm-md-MD_A-ma-1)#map vlan 100
DeviceE(config-cfm-md-MD_A-ma-1)#mep mep-id 5001 interface ge 1/0/4
inward
DeviceE(config-cfm-md-MD_A-ma-1)#end
```

步骤 3 配置连续性检测功能。

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
DeviceA(config-cfm-md-MD_A-ma-1)#ccm send mep-id 1001 enable
DeviceA(config-cfm-md-MD_A-ma-1)#end

DeviceB#configure
```

```
DeviceB(config)#cfm md MD_B
DeviceB(config-cfm-md-MD_B)#ma 2
DeviceB(config-cfm-md-MD_B-ma-2)#ccm send mep-id 2001 enable
DeviceB(config-cfm-md-MD_B-ma-2)#end

DeviceD#configure
DeviceD(config)#cfm md MD_A
DeviceD(config-cfm-md-MD_A)#ma 1
DeviceD(config-cfm-md-MD_A-ma-1)#ccm send mep-id 4002 enable
DeviceD(config-cfm-md-MD_A-ma-1)#end
DeviceD#configure
DeviceD(config)#cfm md MD_B
DeviceD(config-cfm-md-MD_B)#ma 2
DeviceD(config-cfm-md-MD_B-ma-2)#ccm send mep-id 4001 enable
DeviceD(config-cfm-md-MD_B-ma-2)#end

DeviceE#configure
DeviceE(config)#cfm md MD_A
DeviceE(config-cfm-md-MD_A)#ma 1
DeviceE(config-cfm-md-MD_A-ma-1)#ccm send mep-id 5001 enable
DeviceE(config-cfm-md-MD_A-ma-1)#end
```

步骤 4 验证环回功能。

在 Device A 上启用环回功能，检查 MA 1 内 MEP 1001 到 5001 的链路状况。

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
DeviceA(config-cfm-md-MD_A-ma-1)#ping mep-id 1001 rmep-id 5001 count 5
tlv-type null tlv-len 50 priority 0

Pinging 00-03-56-00-00-05 with tlv len 50 of data:
Reply from 00-03-56-00-00-05: bytes=59 time=2ms
Reply from 00-03-56-00-00-05: bytes=59 time=3ms
Reply from 00-03-56-00-00-05: bytes=59 time=2ms
Reply from 00-03-56-00-00-05: bytes=59 time=3ms
Reply from 00-03-56-00-00-05: bytes=59 time=2ms

Packets: Sent = 5, Received = 5, Lost = 0 <0.00% loss>
Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

步骤 5 验证链路跟踪功能。

在 Device A 的 MA 1 内查找 MEP 1001 到 5001 的路径。

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
DeviceA(config-cfm-md-MD_A-ma-1)#trace mep-id 1001 rmep-id 5001 ttl 16
fdb 0

Tracing the route to 00-03-56-00-00-05 over a maximum of 16 hops:
Hop-Num   TTL    MAC              Last-MAC          Ismep   Relay Action
1        15     0003:5600:0005     0003:5600:0001     IsMep   Hit
```

步骤 6 验证单向丢包测试功能。

在 Device A 上测试 MA 1 内 MEP 1001 到 4002 的单向丢包情况。

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
DeviceA(config-cfm-md-MD_A-ma-1)#loss-measure mep-id 1001 rmep-id 4002
interval 1s priority 0 count 5
Info: Single-ended loss measurement will take some time.

Single-ended loss measurement statistics for remote mep 4002 in md MD_A
ma 1:
Packets: Sent = 5, Received = 5, Lost = 0
Far-end frame loss rate : Minimum = 0%, Maximum = 0%, Average = 0%
Near-end frame loss rate: Minimum = 0%, Maximum = 0%, Average = 0%
```

步骤 7 验证双向时延测试功能。

在 Device A 上测试 MA 1 内 MEP 1001 到 4002 的双向时延。

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
DeviceA(config-cfm-md-MD_A-ma-1)#delay-measure mep-id 1001 rmep-id 4002
interval 1s priority 0 frame-len 64 count 5
Info: Two-way delay measurement will take some time.

Two-way delay measurement statistics for remote mep 4002 in md MD_A ma 1:
Packets: Sent = 5, Received = 5, Lost = 0
Delay Time    : Minimum = 1396455us, Maximum = 2219010us, Average =
1785922us
Delay variation: Minimum = 146221us, Maximum = 707088us, Average =
436789us
```

检查结果

通过 **show cfm config** 命令查看 CFM 配置是否正确。

```
DeviceA#show cfm config
!
cfm start
cfm md MD_A level 5 format none
 mip create-type none
 ma 1 format icc 1
  map vlan 100
  mep mep-id 1001 interface ge 1/0/1 inward
  ccm send mep-id 1001 enable
```

8 安全性

本章介绍安全特性的基本原理和配置过程，并提供相关的配置案例。

- ACL
- AAA
- 802.1x
- 安全 MAC
- PPPoE+
- 风暴抑制
- ARP 防攻击
- ND Snooping
- DHCP Snooping
- IP Source Guard
- CPU 防攻击
- MAC 认证
- DOS 防攻击

8.1 ACL

8.1.1 简介

ACL（Access Control List，访问控制列表）是一系列有序规则的集合，通过应用这些规则控制设备接收或拒绝某些数据报文。

在网络中为了控制非法报文对网络的影响，需要在设备上配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过 ACL 定义的。

访问控制列表是由 permit | deny 语句组成的一系列有顺序的规则，这些规则根据数据包的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、端口号等来描述。设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

Management ACL （Management Access Control List，管理访问控制列表）是一系列有序规则的软件规则集合,通过应用这些规则控制设备接收或拒绝某些 IP 访问接入。主要工作在网络的应用层。

在网络中为了控制非法 IP 访问接入（telnet，ssh，ftp，web 等），需要在设备上配置一系列的规则，以决定什么样的 IP 地址能够通过，哪些 IP 地址限制通过，这些规则就是通过管理 ACL 定义的。

8.1.2 配置准备

场景

网络设备为了过滤数据包，需要配置 ACL，以识别需要过滤的对象。在识别出特定的对象之后，才能根据预先设定的策略允许或禁止相应的数据包通过，，丢弃动作支持报文上送 CPU。当 ACL 否定目的 MAC 地址后，相应报文的源 MAC 地址不进行学习且不显示。

- L2 ACL：根据数据包二层帧头携带的源 MAC 地址、目的 MAC 地址、二层协议类型等二层信息制定分类规则，ACL 拒绝的目的 MAC 地址报文，源 MAC 地址也不再学习、不显示。
- IPv4 ACL：根据数据包 IP 头所携带的源 IP、目的 IP、承载的协议类型、使用的 TCP 或 UDP 端口号（默认为 0）等数据包的属性信息制定分类规则。
- IPv6 ACL：根据数据包 IP 头所携带源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、使用的 TCP 或 UDP 端口号（默认为 0）等数据包的属性信息制定分类规则。
- Hybrid ACL：根据数据包二层帧头携带的源 MAC 地址、目的 MAC 地址、IP 头所携带的源 IP、目的 IP 等数据包的属性信息制定分类规则。
- UserDefined ACL：可以以报文的报文头为基准，指定从第几个字节开始与掩码进行“与”操作，将从报文提取出来的字符串与用户定义的字符串进行比较，从而找到相匹配的报文，支持匹配以太网帧前 64 字节任意字段的信息。

根据实际场景的差异，应用 ACL 的方式有有如下几种：基于端口的入方向和出方向、基于 VLAN 的入方向和出方向。

前提

无

8.1.3 配置管理 ACL

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX#**management-acl { start | stop }**	开启关闭管理 ACL 功能

步骤	配置	说明
3	JX#**management-acl src-ip** *source-ip/mask* **protocol {telnet | ssh | ftp | tftp | http} action {permit | deny}**	配置管理 ACL 规则
4	JX#**no management-acl src-ip** *source-ip/mask* **protocol {telnet | ssh | ftp | tftp | http}**	删除管理 ACL 规则
5	JX#**show management-acl**	检查管理 ACL 配置规则

8.1.4 配置 ACL

请在设备上进行以下配置。步骤 3～步骤 7 请根据需要选择配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**acl-l2** *acl-number* [**name** *acl-name*] JX(config)#**acl-ipv4** *acl-number* [**name** *acl-name*] JX(config)#**acl-ipv6** *acl-number* [**name** *acl-name*] JX(config)#**acl-hybrid** *acl-number* [**name** *acl-name*] JX(config)#**acl-userdefined** *acl-number* [**name** *acl-name*]	创建 ACL，进入 ACL 配置模式。 • 取值在 1～1000 之间时，进入基本 MAC ACL 配置模式 • 取值在 1001～2000 之间时，进入基本 IPV4 ACL 配置模式 • 取值在 2001～3000 之间时，进入扩展 HYBRID ACL 配置模式 • 取值在 3001～4000 之间时，进入 IPV6 ACL 配置模式 • 取值在 5001～6000 之间时，进入 Userdefined ACL 配置模式

步骤	配置	说明
3	JX(configure-acl-ipv4-*)#**rule** *rule-id* **src-ip** *ip-address* **dst-ip** *ip-address* [**dscp** *dscp-value* | **tos** *tos-vakue* | **ttl** *ttl-value* | **precedence** *precedence-value* | **fragment** | **proto-type** *proto-type-value*] JX(configure-acl-ipv4-*)#**rule** *rule-id* **arp** { **request | response |any** } **src-ip** { *ip-address/ip-address-mask* | *ip-address/ip-address-masklength* | **any** } **dst-ip** { *ip-address/ip-address-mask* | *ip-address/ip-address-masklength* | **any** }JX(configure-acl-ipv4-*)#**rule** *rule-id* **action** { **8021p** *8021p-value* | **cos** *cos-value* | **counter** *counter-id* | **cpu** | **deny** | **dscp** *dscp-value* | **insert-inner-vid** *vlan-id* | **insert-outer-id** *vlan-id* | **mirror group** *group-id* | **permit** | **precedence** *precedence-value* | **redirect** *interface-type interface-number* | **replace-inner-vid** *vlan-id* | **replace-outer-vid** *vlan-id* | **tos** *tos-value* } JX(configure-acl-ipv4-*)#**rule** *rule-id* **cir** { **gbps** | **kbps** | **mbps** } *value* **outaction drop** JX(configure-acl-ipv4-*)#**rule** *rule-id* **meter** *meter-id* **outaction** { **red-drop** [**yellow-drop**] | **yellow-drop** [**red-drop**] } JX(configure-acl-ipv4-*)#**rule** *rule-id* **time-range** *index* JX(configure-acl-ipv4-*)#**rule** *rule-id* **icmp src-ip** *ip-address* **dst-ip** *ip-address* **icmp-type** *icmp-type* **icmp-code** *icmp-code* **[fragment]** JX(configure-acl-ipv4-*)#**rule** *rule-id* **tcp src-ip** *ip-address* **src-port** *port* **dst-ip** *ip-address* **dst-port** *port* **{ syn|synack|ack|fin } [fragment]** JX(configure-acl-ipv4-*)#**rule** *rule-id* **igmp src-ip** *ip-address* **dst-ip** *ip-address* **[fragment]** JX(configure-acl-ipv4-*)#**rule** *rule-id* **udp src-ip** *(ip-address* **src-port** *port* **dst-ip** *ip-address* **dst-port** *port* **[fragment]**	配置 IP ACL 的匹配规则。

步骤	配置	说明
4	JX(configure-acl-l2-*)#**rule** *rule-id* **src-mac** *mac-address* **dst-mac** *mac-address* [**outer-vlan** *vlan* **8021p** *8021p-value* | **inner-vlan** *vlan* **8021p** *8021p-value*] JX(configure-acl-l2-*)#**rule** *rule-id* **src-mac** *mac-address* **dst-mac** *mac-address* **eth-type** **{ ip|arp|<0x0600-0xfffe> }** JX(configure-acl-l2-*)#**rule** *rule-id* **src-mac** *mac-addr* **dst-mac** *mac-address* **{inner-vlan|outer-vlan}** *vlan-id* **8021p** *cos* JX(configure-acl-l2-*)#**rule** *rule-id* **action** { **8021p** *8021p-value* | **cos** *cos-value* | **counter** *counter-id* | **cpu** | **deny** | **dscp** *dscp-value* | **insert-inner-vid** *vlan-id* | **insert-outer-id** *vlan-id* | **mirror group** *group-id* | **permit** | **precedence** *precedence-value* | **redirect** *interface-type interface-number* | **replace-inner inner-vid** *vlan-id* | **replace-outer-vid** *vlan-id* | **tos** *tos-value* } JX(configure-acl-l2-*)#**rule** *rule-id* **cir** { **gbps** | **kbps** | **mbps** } *value* **outaction drop** JX(configure-acl-l2-*)#**rule** *rule-id* **meter** *meter-id* **outaction** { **red-drop** [**yellow-drop**] | **yellow-drop** [**red-drop**] } JX(configure-acl-l2-*)#**rule** *rule-id* **time-range** *index*	配置 MAC ACL 的规则。

步骤	配置	说明
5	JX(configure-acl-ipv6-*)#**rule** *rule-id* **src-ip** *ipv6-address* **dst-ip** *ipv6-address* [**hop-limit** *hot-limit-value* | **next-header** *next-header-value* | **traffic-class** *traffic-class-value*] JX(configure-acl-ipv6-*)#**rule** *rule-id* **tcp src-ip** *ipv6-address* **src-port** *port* **dst-ip** *ipv6-address* **dst-port** *port* **[syn|synack|ack|fin|fragment]** JX(configure-acl-ipv6-*)# **rule** *rule-id* **udp src-ip** *ipv6-address* **src-port** *port* **dst-ip** *ipv6-address* **dst-port** *port* [**fragment**] JX(configure-acl-ipv6-*)#**rule** *rule-id* **icmp src-ip** { *ipv6-address* | **any** } **dst-ip** { *ipv6-address* | **any** } **icmp-type** *icmp-type* **icmp-code** *icmp-code* **[fragment]** JX(configure-acl-ipv6-*)#**rule** *rule-id* **igmp src-ip** { *ipv6-address* | **any** } **dst-ip** { *ipv6-address* | **any** } **[fragment]** JX(configure-acl-ipv6-*)#**rule** *rule-id* **action** { **8021p** *8021p-value* | **cos** *cos-value* | **counter** *counter-id* | **cpu** | **deny** | **dscp** *dscp-value* | **insert-inner-vid** *vlan-id* | **insert-outer-id** *vlan-id* | **mirror group** *group-id* | **permit** | **precedence** *precedence-value* | **redirect** *interface-type interface-number* | **replace-inner -vid** *vlan-id* | **replace-outer-vid** *vlan-id* | **tos** *tos-value* } JX(configure-acl-ipv6-*)#**rule** *rule-id* **cir** { **gbps** | **kbps** | **mbps** } *value* **outaction drop** JX(configure-acl-ipv6-*)#**rule** *rule-id* **meter** *meter-id* **outaction** { **red-drop** [**yellow-drop**] | **yellow-drop** [**red-drop**] } JX(configure-acl-ipv6-*)#**rule** *rule-id* **time-range** *index*	配置 IPv6 ACL 的规则。

步骤	配置	说明
6	JX(configure-acl-hybrid-*)#**rule** *rule-id* **action** { **8021p** *8021p-value* | **cos** *cos-value* | **counter** *counter-id* | **cpu** | **deny** | **dscp** *dscp-value* | **insert-inner-vid** *vlan-id* | **insert-outer-id** *vlan-id* | **mirror group** *group-id* | **permit** | **precedence** *precedence-value* | **redirect** *interface-type interface-number* | **replace-inner -vid** *vlan-id* | **replace-outer-vid** *vlan-id* | **tos** *tos-value* } JX(configure-acl- hybrid -*)#**rule** *rule-id* **arp** { **request | response |any** } **src-ip** { *ip-address/ip-address-mask* | *ip-address/ip-address-masklength* | **any** } **dst-ip** { *ip-address/ip-address-mask* | *ip-address/ip-address-masklength* | **any** } JX(configure-acl- hybrid -*)#**rule** *rule-id* **cir** { **gbps** | **kbps** | **mbps** } *value* **outaction drop** JX(configure-acl- hybrid -*)#**rule** *rule-id* **icmp src-ip** *ip-address* **dst-ip** *ip-address* **icmp-type** *icmp-type* **icmp-code** *icmp-code* **[fragment]** JX(configure-acl- hybrid -*)#**rule** *rule-id* **igmp src-ip** *ip-address* **dst-ip** *ip-address* **[fragment]** JX(configure-acl- hybrid -*)#**rule** *rule-id* **meter** *meter-id* **outaction** { **red-drop** [**yellow-drop**] | **yellow-drop** [**red-drop**] } JX(configure-acl- hybrid -*)#**rule** *rule-id* **src-ip** *ip-address* **dst-ip** *ip-address* [**dscp** *dscp-value* | **tos** *tos-vakue* | **ttl** *ttl-value* | **precedence** *precedence-value* | **fragment** | **proto-type** *proto-type-value*] JX(configure-acl- hybrid -*)#**rule** *rule-id* **src-mac** *mac-address* **dst-ip** *mac-address* **eth-type** {*<0×0600-0×fffe>* | **arp** | **ip** | **any** } **outer-vlan** *vlan-id* **8021p** *dot1p-value* **inner-vlan** *inner-vlan-id* **8021p** *dot1p-value* **src-ip** *srp-ip-address* **dst-ip** *dst-ip-address* **proto-type** { { *value* **| any** } | { **tcp** | **udp** } **src-port** { *source-number* | **any** } **dst-port** { *destination-number* | **any** } } JX(configure-acl- hybrid -*)#**rule** *rule-id* **src-mac** *mac-address* **dst-ip** *mac-address* **inner-vlan** { *inner-vlan-id* | **any** } **8021p** { *dot1p-value* | **any** } JX(configure-acl- hybrid -*)#**rule** *rule-id* **src-mac** *mac-address* **dst-ip** *mac-address* **outer-vlan** { *outer-vlan-id* | **any** } **8021p** { *dot1p-value* | **any** } [**inner-vlan** { *inner-vlan-id* | **any** } **8021p** { *dot1p-value* | **any** }] JX(configure-acl- hybrid -*)#**rule** *rule-id* **tcp src-ip** *ip-address* **src-port** *port* **dst-ip** *ip-address* **dst-port** *port* [{ **syn|synack|ack|fin** } [**fragment**]]	配置 Hybrid 的规则。
	JX(configure-acl- hybrid -*)#**rule** *rule-id* **time-range** *index* JX(configure-acl- hybrid -*)#**rule** *rule-id* **udp src-ip** *(ip-address* **src-port** *port* **dst-ip** *ip-address* **dst-port** *port* **[fragment]**	

步骤	配置	说明
7	JX(configure-acl-userdefined-*)#**rule** *rule-id* **action** { **8021p** *8021p-value* | **cos** *cos-value* | **counter** *counter-id* | **cpu** | **deny** | **dscp** *dscp-value* | **insert-inner-vid** *vlan-id* | **insert-outer-id** *vlan-id* | **mirror group** *group-id* | **permit** | **precedence** *precedence-value* | **redirect** *interface-type interface-number* | **replace-inner-vid** *vlan-id* | **replace-outer-vid** *vlan-id* | **tos** *tos-value* } JX(configure-acl-userdefined-*)#**rule** *rule-id* **cir** { **gbps** | **kbps** | **mbps** } *value* **outaction drop** JX(configure-acl-userdefined-*)#**rule** *rule-id* **meter** *meter-id* **outaction** { **red-drop** [**yellow-drop**] | **yellow-drop** [**red-drop**] } JX(configure-acl-ipv4-*)#**rule** *rule-id* **time-range** *index*	配置 userdefined 规则。
7	JX(configure-acl-ipv4-*)#**rule** *rule-id* **action** **{permit|deny|mirror|redirect|counter}**	配置基本 IP ACL 的动作。

8.1.5 应用 ACL

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或者 VLAN 配置模式，以下以物理接口模式为例进行说明。
3	JX(config-ge-1/0/*)#**acl-l2** { **in** | **out** } *acl-num*	在接口上应用 ACL。
	JX(config-ge-1/0/*)#**acl-l2** { **in** | **out** }*name*	在接口上应用 ACL。
4	JX(config-ge-1/0/*)#**exit**	返回全局配置模式。

8.1.6 配置统计

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**counter** *counter-id* **{packet|byte|all} sort { green | greenred | greenyellow | red | redyellow | total }**	创建统计模版
3	JX(configure-acl-l2-*)#**rule** *rule-id* **action counter** *counter-id*	在 acl 中应用统计模版

8.1.7 配置限速

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**meter** *<1-128>* **pps** *<1-1000000>* **color { aware | blind }**	创建基于包个数的限速模版
3	JX(config)#**meter** *<1-128>* **cir { kbps | mbps | gbps }** *cir-value* **cbs { bytes | kbytes | mbytes }** *cbs-value* **ebs { bytes | kbytes | mbytes }** *ebs-value* **color { aware | blind }**	创建单速三色的限速模版
4	JX(config)#**meter** *<1-128>* **cir { kbps | mbps | gbps }** *cir-value* **cbs { bytes | kbytes | mbytes }** *cbs-value* **pir { kbps | mbps | gbps }** *pir-value* **pbs { bytes | kbytes | mbytes }** *pbs-value* **color { aware | blind }**	创建双速三色的限速模版
3	JX(configure-acl-l2-*)#**rule** *rule-id* **meter** *meter-id* **outaction { red-drop | yellow-drop }**	在 acl 中应用限速模版

8.1.8 配置时间段

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**time-range list** *id*	创建时间段
3	JX(config-timerange-*)#**time-range** *timerange-id* **absolute from** *hour:minute:second year/month/monthday* **to** *hour:minute:second year/month/monthday* JX(config-timerange-*)#**time-range** *timerange-id* **everyhour** *minute:second* **to** *minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyday** *hour:minute:second* **to** *hour:minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyweek** *hour:minute:second* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } **to** { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } JX(config-timerange-*)#**time-range** *timerange-id* **everymonth** *hour:minute:second monthday* **to** *hour:minute:second monthday* JX(config-timerange-*)#**time-range** *timerange-id* **everyweekend** *hour:minute:second* **to** *hour:minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyyear** *hour:minute:second month/monthday* **to** *hour:minute:second month/monthday*	创建时间段，可应用于 ACL 规则。 对时间段（周期时间段）：是指 everyxxx 描述的以一周为间隔的期性时间，同时可以依靠绝对时段指明时间范围有效日期。 对时间段：是指由 absolute 指定特定的时间范围。可以通过绝对间段指定的时间范围来限制相对间段（周期时间段）在什么时间围生效。 果该时间段配置了多个生效时，生效原则为：周期时间段之间“或”，周期时间段和绝对时间段间取“与”
4	JX(configure-acl-l2-*)#**rule** *rule-id* **time-range** *timerange-list-id*	在 acl 中应用时间段

8.1.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show acl config**	查看 ACL 配置信息。
2	JX#**show acl interface**	查看接口 acl 配置信息。
3	JX#**show acl statistics**	查看 acl 统计信息。
4	JX#**show time-range list**	查看时间段配置相关信息。

8.1.10 维护

用户可以通过以下命令，维护设备 ACL 特性的运行情况和配置情况。

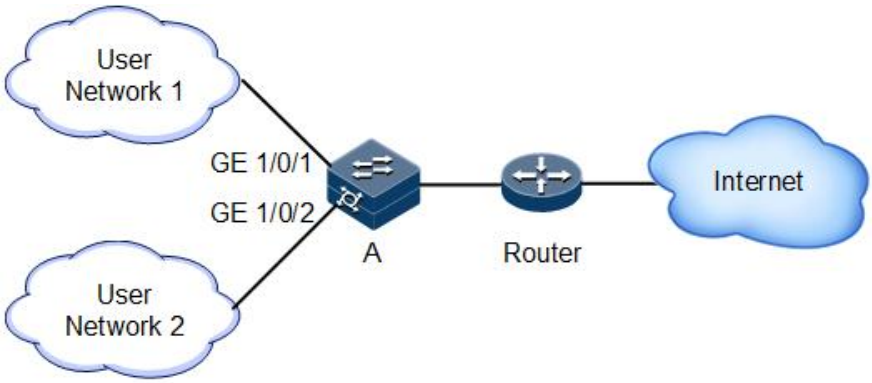
命令	描述
JX(config)#**reset acl statistics [acl** *acl-id* **|rule** *rule-id* **| direction {in|out}]**	清除全局 ACL 统计信息。
JX(config)#**reset acl statistics interface** *interface-type interface-number* **[acl** *acl-id* **|rule** *rule-id* **|direction {in|out}]**	清除接口 ACL 统计信息。

8.1.11 配置 ACL 示例

组网需求 1

如下图所示，想要控制在每天 00:00 到 08:00 之间，拒绝通过 SwitchA 访问互联网的请求，在每天 08:00 到 12:00 之间，限制访问速度为 10000pps

图 8-1 ACL 示例



配置步骤

步骤 1 配置 timerange。

```
JX#configure
JX(config)#timerange list 1
JX(config-timerange-1)#time-range 1 everyday 00:00:00 to 08:00:00
JX(config-timerange-1)#configure
JX(config)#timerange list 2
JX(config-timerange-1)#time-range 1 everyday 08:00:00 to 12:00:00
```

步骤 2 配置 meter。

```
JX#configure
JX(config)#meter 1 pps 10000 color blind
```

步骤 3 配置 acl 匹配规则和动作。

```
JX#configure
JX(config)#acl-l2 1 name test
JX(configure-acl-l2-1)#rule 1 src-mac any dst-mac any
JX(configure-acl-l2-1)#rule 1 time-range 1
JX(configure-acl-l2-1)#rule 1 action deny
JX(configure-acl-l2-1)#rule 2 src-mac any dst-mac any
JX(configure-acl-l2-1)#rule 2 time-range 2
JX(configure-acl-l2-1)#rule 2 meter 1 outaction red-drop yellow-drop
```

步骤 4 在接口上应用 acl。

```
JX#configure
JX(config)#interface ge 1/0/1 to ge 1/0/2
JX(config-ge-1/0/1->ge-1/0/2)#acl-l2 in 1
```

检查结果

```
JX#show acl config
!
acl-l2 1 name test
 rule 1 src-mac any dst-mac any
 rule 1 time-range 1
 rule 1 action deny
 rule 2 src-mac any dst-mac any
 rule 2 time-range 2
 rule 2 meter 1 outaction red-drop yellow-drop
!
interface ge 1/0/1
 acl-l2 in name test
!
interface ge 1/0/2
 acl-l2 in name test
```

组网需求 2

如图 8-1 所示，客户想要对 SwitchA 上不同接口，VLAN 和 8021p 优先级的数据，进行分类，执行不同的动作。从 GE 1/0/1 接口来的流量，修改 DSCP 为 46，从 GE 1/0/2 接口来的 VLAN 100 的流量，提高 8021p 优先级为 7。

配置步骤

步骤 1 配置 acl 匹配规则和动作。

```
JX#configure
JX(config)#acl-l2 1 name test
JX(configure-acl-l2-1)#rule 1 src-mac any dst-mac any
JX(configure-acl-l2-1)#rule 1 action dscp 46
JX(configure-acl-l2-1)#configure
JX(config)#acl-l2 2 name test2
JX(configure-acl-l2-2)#rule 1 src-mac any dst-mac any outer-vlan 100
8021p any
JX(configure-acl-l2-2)#rule 1 action 8021p 7
```

步骤 2 在接口上应用 acl。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#acl-l2 in 1
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#acl-l2 in 2
```

检查结果

```
JX#show acl config
!
acl-l2 1 name test
 rule 1 src-mac any dst-mac any
  rule 1 action dscp 46
acl-l2 2 name test2
 rule 1 src-mac any dst-mac any outer-vlan 100 8021p any
  rule 1 action 8021p 7
!
interface ge 1/0/1
 acl-l2 in name test
!
interface ge 1/0/2
 acl-l2 in name test2
```

8.2 AAA

8.2.1 简介

AAA

AAA（Authentication、Authorization、Accounting，认证、授权、计费）是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

- 认证：确认访问网络的远程用户的身份，判断访问者是否为合法的网络用户。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。例如，管理员授权办公用户才能对服务器中的文件进行访问和打印操作，而其它临时访客不具备此权限。
- 计费：记录用户使用网络服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对时间、流量的计费需求，也对网络起到监视作用。

AAA 采用客户端/服务器结构，客户端运行于 NAS（Network Access Server，网络接入服务器）上，负责验证用户身份与管理用户接入，服务器上则集中管理用户信息。

AAA 可以通过多种协议来实现，这些协议规定了 NAS 与服务器之间如何传递用户信息。目前设备支持 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）协议和 TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）。

RADIUS

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）是一种用于对远程访问用户进行集中鉴别的标准化通信协议。RADIUS 使用 UDP 作为传输协议（端口 1812、1813），具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。

- 认证功能

RADIUS 使用客户端/服务器模式，网络访问设备作为 RADIUS 服务器的客户端。RADIUS 服务器负责接收用户的连接请求、对用户进行鉴别，然后将所有客户端所需的配置信息传回，以便为用户提供服务。通过这种方式可以控制用户对设备和网络的访问，提高网络的安全性。

客户端与 RADIUS 服务器之间的通信是通过共享密钥的使用来鉴别的，这个共享密钥不会通过网络传送。此外，任何用户口令在客户机和 RADIUS 服务器间发送时都需要进行加密过程，以避免有人通过嗅探非安全网络得到用户密码。

- RADIUS 计费功能

RADIUS 计费功能主要针对通过 RADIUS 认证的用户进行。在用户登录时给 RADIUS 计费服务器发送一个开始计费的报文，在登录期间根据计费策略给 RADIUS 计费服务器发送计费更新报文，退出登录时，给 RADIUS 计费服务器发送停止计费报文，报文里面包含用户的登录时间。通过这些报文，RADIUS 计费服务器可以记录每个用户的访问时间和操作。

TACACS+

TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）是一种与 RADIUS 类似的网络接入认证协议。其区别如下：

- TACACS+使用 TCP 端口 49，相对于 RADIUS 使用的 UDP 端口，具有更高的传输可靠性。
- TACACS+加密数据包除标准的 TACACS+头部外的整体，而包头中有一个区域会指示数据包是否加密。相对于 RADIUS 的只加密用户密码，安全性更高。
- TACACS+的认证功能与授权、计费功能相分离，部署更灵活。

综上所述，TACACS+较 RADIUS 更加安全、可靠，但是 RADIUS 作为一种开放性的协议，在网络中的应用更加广泛。

8.2.2 配置准备

场景

为了控制用户对设备和网络的访问，可以在网络中部署 RADIUS/TACACS+服务器对用户进行认证和计费。本设备可以作为 RADIUS/TACACS+服务器的代理设备，根据 RADIUS/TACACS+服务器反馈的结果对用户访问进行授权。TACACS+较 RADIUS 更加安全、可靠。

前提

无

8.2.3 缺省配置

设备上 AAA 的缺省配置如下。

功能	缺省值
RADIUS 认证服务器未响应之后的失效时间	60 秒
RADIUS 报文重传次数	3
RADIUS 报文重传时间间隔	2 秒
RADIUS 认证服务器未响应之后的失效时间	60 秒
TACACS 认证服务器 TCP 连接超时和收包超时时间	2 秒

8.2.4 配置 RADIUS 服务器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**radius-server deadtime** { *second* | **default** }	全局配置服务器未响应之后的失效时间，取值范围为 3～4294967290，单位为秒，缺省值为 60 秒。
4	JX(config-aaa)#**radius-server max-retransmit** { *count* | **default** }	全局配置发送请求失败后的重传次数，取值范围为 1～5，缺省值为 3 次。
5	JX(config-aaa)#**radius-server retransmit-interval** { *interval* | **default** }	全局配置重传时间间隔，取值范围为 1～10，缺省值为 2 秒。
6	JX(config-aaa)#**radius-server host** *server-name* **ip-address** *ip-address* **key** *key* [**acct-port** *port-id* | **auth-port** *port-id* | **deadtime** { *second* | **default** } | **max-retransmit** { *count* | **default** } | **retransmit-interval** { *interval* | **default** } | **source-ip** *ip-address*]	创建 IPv4 RADIUS 服务器。

步骤	配置	说明
7	JX(config-aaa)#**radius-server host** *server-name* **ip6-address** *ipv6-address* **key** *key* [**acct-port** *port-id* | **auth-port** *port-id* | **deadtime** { *second* | **default** } | **max-retransmit** { *count* | **default** } | **retransmit-interval** { *interval* | **default** } | **source-ip6** *ipv6-address*]	创建 IPv6 RADIUS 服务器。

8.2.5 配置 TACACS+服务器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**tacacs-server deadtime** { *second* | **default** }	全局配置服务器未响应之后的失效时间，取值范围为 3～4294967290，单位为秒，缺省值为 60 秒。
4	JX(config-aaa)#**tacacs-server timeout** { *second* | **default** }	全局配置与服务器的 TCP 连接超时和收包超时时间，缺省值为 2 秒。
5	JX(config-aaa)#**tacacs-server host** *server-name* **ip-address** *ip-address* **key** *key* [**deadtime** { *second* | **default** } | **port** *port-id* | **single-connection** { **enable** | **disable** } | **timeout** { *second* | **default** } | **source-ip** *ip-address*]	创建 IPv4 TACACS 服务器。
6	JX(config-aaa)#**tacacs-server host** *server-name* **ip6-address** *ipv6-address* **key** *key* [**deadtime** { *second* | **default** } | **port** *port-id* | **single-connection** { **enable** | **disable** } | **timeout** { *second* | **default** } | **source-ip6** *ipv6-address*]	创建 IPv6 TACACS 服务器。

8.2.6 配置 AAA 服务器组

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**aaa**	进入 AAA 配置模式。

步骤	配置	说明
3	JX (config-aaa)#**server-group** *group-name* { **radius-server** | **tacacs-server** } *server-name*	创建 AAA 服务器组或向 AAA 服务器组添加服务器

8.2.7 配置 AAA 方法

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**aaa authentication** { **dot1x** | **login** | **mac-authen** | **enable** } **method** *method-name* **first** { *group-name* | **local** } **second** { *group-name* | **local** | **none** } **third** { *group-name* | **local** | **none** }	配置 AAA 认证方法。 注意事项：服务器组最多配置两个。
4	JX(config-aaa)#**aaa authorization** { **login** | **cmd** } **method** *method-name* **first** { *group-name* | **local** } **second** { *group-name* | **local** | **none** } **third** { *group-name* | **local** | **none** }	配置 AAA 授权方法。 注意事项：服务器组最多配置两个。
5	JX (config-aaa)#**aaa accounting** { **dot1x** | **login** | **mac-authen** } **method** *method-name* **first** { *group-name* | **local** } **second** { *group-name* | **local** | **none** } **third** { *group-name* | **local** | **none** }	配置 AAA 计费方法。 注意事项：服务器组最多配置两个。

8.2.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show aaa config**	查看 AAA 配置信息。
2	JX#**show aaa information**	查看 AAA 全局信息。
3	JX#**show aaa server**	查看 AAA 服务器信息。
4	JX#**show aaa server-group**	查看 AAA 服务器组信息。
5	JX#**show aaa method**	查看 AAA 方法信息。

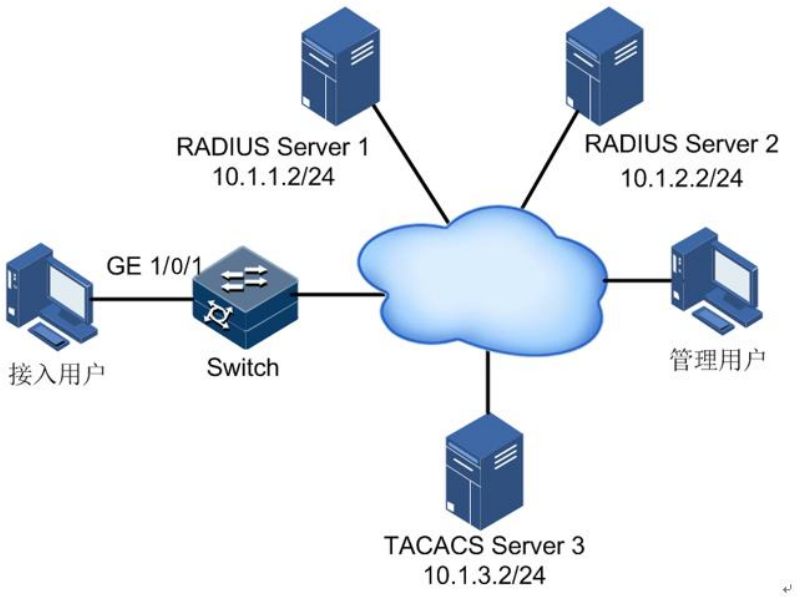
8.2.9 配置 AAA 示例

组网需求

如下图所示，实现接入用户和管理用户接入不同的服务器，要求配置如下：

- 在 Switch 上配置 IP 地址、Vlan 和路由，用于用户连接及认证。
- 创建本地用户，配置管理用户所用的 AAA 模板和方案，采用 TACACS Server 3 进行认证和授权，RADIUS Server 2 进行计费。
- 开启 Dot1x 功能，配置接入用户所使用的 AAA 模板和方案，采用 RADIUS Server 1 进行认证、计费和授权。

图 8-2 分域认证应用组网示意图



配置步骤

步骤 1 配置 IP 地址。

```
JX#config
JX(config)#interface vlan 1
JX(config-vlanif-1)#ip address 10.1.0.254/24
JX(config-vlanif-1)#exit
JX(config)ip route-static 0.0.0.0 0.0.0.0 10.1.0.1
```

步骤 2 配置 AAA 服务器。

```
JX(config)#aaa
JX(config-aaa)#radius-server host Server1 ip-address 10.1.1.2
JX(config-aaa)#radius-server host Server2 ip-address 10.1.2.2
JX(config-aaa)#tacacs-server host Server3 ip-address 10.1.3.2
```

步骤 3 配置 AAA 服务器组。

```
JX(config-aaa)#server-group Group1 radius-server Server1
JX(config-aaa)#server-group Group2 radius-server Server2
JX(config-aaa)#server-group Group3 tacacs-server Server3
```

步骤 4 配置 AAA 方法。

```
JX(config-aaa)#aaa authentication login method Method1 first Group3
JX(config-aaa)#aaa authorization login method Method2 first Group3
JX(config-aaa)#aaa accounting login method Method3 first Group2
JX(config-aaa)#aaa authentication dot1x method Method4 first Group1
JX(config-aaa)#aaa accounting dot1x method Method5 first Group1
JX(config-aaa)#exit
```

步骤 5 配置管理用户认证、授权、计费方法。

```
JX(config)#line vty 1 2
JX(config-line)#login authentication aaa method Method1
JX(config-line)#login authorization aaa method Method2
JX(config-line)#login accounting aaa method Method3
JX(config-line)#exit
```

步骤 6 配置接入用户认证、授权、计费方法。

```
JX(config)#dot1x start
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dot1x enable
JX(config-ge-1/0/1)#dot1x aaa authentication method Method4
JX(config-ge-1/0/1)#dot1x aaa accounting method Method5
JX(config-ge-1/0/1)#exit
```

检查结果

步骤 1 通过 **show aaa config** 查看 AAA 配置是否正确。

```
JX#show aaa config
Version  : AAA_V7.00.00.00
!
aaa
 radius-server host Server1 ip-address 10.1.1.2
 radius-server host Server2 ip-address 10.1.2.2
 tacacs-server host Server3 ip-address 10.1.3.2
 server-group Group1 radius-server Server1
 server-group Group2 radius-server Server2
 server-group Group3 tacacs-server Server3
 aaa authentication login method Method1 first Group3
 aaa authorization login method Method2 first Group3
 aaa accounting login method Method3 first Group2
 aaa authentication dot1x method Method4 first Group1
 aaa accounting dot1x method Method5 first Group1
```

8.3 802.1x

8.3.1 简介

802.1x 是基于 IEEE 802.1x 协议即基于接口的网络接入控制技术。802.1x 功能的主要目的是解决局域网用户的接入认证和安全问题。

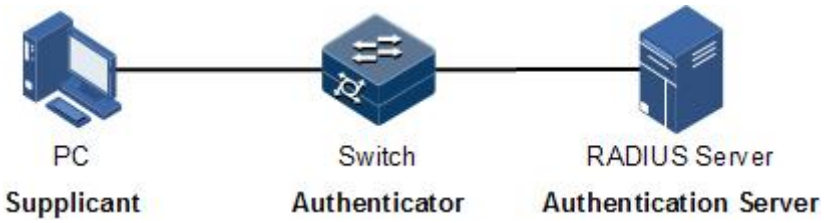
在网络设备的物理接入层对接入设备进行认证和控制，仅定义了设备接口和用户设备之间的点到点连接方式。连接在接口上的用户设备如果能够通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法通过交换机访问网络中的资源。

802.1x 体系结构

802.1x 认证采用客户端/服务器模式，如下图所示，包括以下 3 个部分：

- 申请者（Supplicant）：需要安装 802.1x 客户端软件（例如 Windows XP 自带的 802.1x 客户端）的用户侧设备，如计算机等。
- 认证者（Authenticator）：提供 802.1x 认证功能的接入控制设备，如交换机等。
- 认证服务器（Authentication Server）：用于对用户进行认证、授权和计费，通常使用 RADIUS 服务器作为 802.1x 认证服务器。

图 8-3 802.1x 认证体系结构



接口接入控制模式

认证者利用认证服务器对需要接入局域网的客户端进行认证，并根据认证结果对接入接口授权或者非授权状态进行控制。用户可以通过配置接口的接入控制模式来控制接口的接入状态。802.1x 认证支持三种接口接入控制模式：

- 协议授权模式（auto）：由协议状态机决定认证授权结果，在认证成功之前，仅允许收发 EAPoL 报文，不允许用户访问网络资源和交换机提供的服务。如果认证通过，则接口切换到授权状态，允许用户访问网络资源和交换机提供的服务。
- 强制接口授权模式（authorized-force）：接口始终处于授权状态，允许用户不经认证授权即可访问网络资源和交换机提供的服务。
- 强制接口非授权模式（unauthorized-force）：接口始终处于非授权状态，不允许用户访问网络资源和交换机提供的服务，即不允许用户进行认证。

802.1x 认证过程

802.1x 系统支持 EAP 中继和 EAP 终结两种方式完成与 RADIUS 服务器之间的认证过程。

- EAP 中继方式

申请者与认证服务器之间通过 EAP（Extensible Authentication Protocol，可扩展认证协议）报文交换信息。申请者与认证者之间则以 IEEE802.1x 协议所定义的 EAPoL（EAP over LAN，基于局域网的 EAP）报文交换信息。EAP 报文中封装了认证数据，该认证数据将被封装在 RADIUS 协议的报文中，以穿越复杂的网络到达认证服务器，这一过程称为 EAP 中继。

认证者或申请者均能发起 802.1x 认证过程。以申请者发起认证过程为例，EAP 中继认证过程如下：

1. 用户输入用户名和密码，申请者向认证者发送一个 EAPoL-Start 报文，开始一次 802.1x 认证；
2. 认证者向申请者发送 EAP-Request/Identity 报文，询问请求者的用户名；
3. 申请者响应一个 EAP-Response/Identity 给认证者，其中包括用户名信息；
4. 认证者将 EAP-Response/Identity 报文封装到 RADIUS 协议报文中，发送给认证服务器；
5. 认证服务器将接收到的用户名信息与数据库中的用户名表进行比对，找到该用户的口令信息，利用随机生成的加密字对口令信息进行加密处理。同时，认证服务器将此加密字发送给认证者，认证者再将此加密字发送给申请者；
6. 申请者利用接收到的加密字对口令进行加密，并通过认证者发送给认证服务器；
7. 认证服务器对比收到的加密口令与自身生成的加密口令否一致。如果认证成功，认证者将接口改为授权状态，允许用户通过接口访问网络，并发送 EAP-Success 报文给申请者；如果认证失败，则接口为非授权状态，并发送 EAP-Failure 报文给通知申请者。

- EAP 终结方式

将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费过程。设备端支持与 RADIUS 服务器之间采用 PAP 或者 CHAP 认证方法。

在 EAP 终结方式中，用来对用户密码信息进行加密处理的随机加密字由设备端生成，之后设备端会把用户名、随机加密字和客户端加密后的密码信息共同发送给 RADIUS 服务器，进行相关的认证处理。

802.1x 定时器

802.1x 认证过程中，认证设备上涉及到 5 个定时器：

- Reauth-period：重认证定时器。在该定时器超时后，会重新发起 802.1x 认证。
- Quiet-period：静默定时器。用户认证失败以后，认证设备需要静默一段时间，静默定时器超时后再重新发起认证。在静默期间，交换机不处理认证报文。

- Tx-period：请求报文发送超时定时器。当交换机向用户请求端发送 Request/Identity 请求报文后，会启动该定时器，在该定时器超时后，用户端软件未成功发送认证应答报文，则设备重发认证请求报文，此报文共重发 3 次。
- Supp-timeout：申请者认证超时定时器。当交换机向用户请求端发送了用于请求用户端 MD5 加密密文的 Request/Challenge 请求报文后，交换机启动该定时器。若在该定时器设置的时长内用户请求端未成功响应，交换机将重发该报文，此报文共重发两次。
- Server-timeout：认证服务器超时定时器。该定时器定义认证者和认证服务器会话超时的总时长，此定时器超时后认证者结束同认证服务器会话，重新开始一次新的认证过程。

802.1x guest-vlan

在网络中，用户在未经过 802.1x 认证时只能访问有限资源，当配置 guest-vlan 功能后，设备对 untag 报文添加 guest-vlan，并允许该报文通过端口。

- 基于端口认证：认证时认证通过会删除端口的 guest-vlan。
- 基于用户认证：认证通过会保留端口的 guest-vlan。
- guset-vlan 不能是 supervlan，也不能是 voice-vlan。

8.3.2 配置准备

场景

为了实现对局域网用户的接入认证，并解决接入用户的安全问题，需要在设备上配置 802.1x 认证。

对于认证通过的用户，允许其访问网络中的资源；如果认证未通过，则该用户无法访问网络资源。通过对用户接入接口的认证控制，达到对用户管理的目的。

前提

配置 802.1x 认证之前，如果使用 RADIUS 认证服务器，需要完成以下任务：

- 配置 RADIUS 服务器 IP 地址和 RADIUS 公有密钥。
- 交换机能够与 RADIUS 服务器 Ping 通。

8.3.3 802.1x 功能的缺省配置

设备上 802.1x 功能的缺省配置如下。

功能	缺省值
全局 802.1x 功能状态	禁止
接口 802.1x 功能状态	禁止
全局认证方式	**chap**
接口接入控制模式	**auto**

功能	缺省值
接口认证方式	**macbased**
RADIUS 服务器超时定时器时间	10s
802.1x 重认证功能状态	允许
802.1x 重认证定时器时间	3600s
802.1x 静默定时器时间	60s
请求报文重传定时器时间	30s
最大用户数	128

8.3.4 配置 802.1x 基本功能

注意

- 一个接口同一时刻只能处理一个用户认证请求。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dot1x { start | stop }**	使能或去使能全局 802.1x 功能。
3	JX(config)#**dot1x aaa authentication method** *method-name*	绑定全局 802.1x 认证时的 AAA 方法。
4	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
5	JX(config-ge-1/0/*)#**dot1x enable**	使能接口 802.1x 功能。
6	JX(config-ge-1/0/*)#**dot1x port-control { auto | force-auth | force-unauth }**	配置接口接入控制模式。
7	JX(config-ge-1/0/*)#**dot1x port-method { mac | port }**	配置接口认证方式。
8	JX(config-ge-1/0/*)#**dot1x max-user** *user-number*	配置 802.1x 端口允许认证的最大用户数。
9	JX(config-ge-1/0/*)#**nac guest-vlan** *vlan-id*	配置指定端口的 Guest VLAN，对 802.1x 协议和 mac 认证都生效。
10	JX(config-ge-1/0/*)#**dot1x critical-vlan** *vlan-id*	配置指定端口的 802.1x Critical VLAN。

步骤	配置	说明
11	JX(config-ge-1/0/*)#**dot1x restrict-vlan** *vlan-id*	配置指定端口的 802.1x Restrict VLAN。
12	JX(config-ge-1/0/*)#**dot1x reauthenticate all user**	手动触发指定端口下 802.1x 用户进行重认证。
13	JX(config-ge-1/0/*)#**dot1x delete all user**	强制将端口下 802.1x 用户下线。
14	JX(config-ge-1/0/*)#**dot1x quiet** { **disable** | **enable** }	使能或去使能端口 802.1x 用户静默功能。
15	JX(config-ge-1/0/*)#**dot1x quiet-times** *times*	配置端口 802.1x 用户触发静默功能的认证失败次数，默认 3 次。

说明

如果全局或接口模式下未使能 802.1x 功能，则接口下不能使能 802.1x 功能。

8.3.5 配置 802.1x 重认证

注意

重认证功能是针对已授权的用户发起的，所以在使能重认证功能之前，应该保证使能全局和接口 802.1x 功能。处于授权状态的接口在重认证过程中仍保持授权状态，如果重认证失败，才进入非授权状态。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**dot1x reauthenticate** { **enable** | **disable** }	使能 802.1x 重认证功能。

8.3.6 配置 802.1x 定时器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**dot1x reauthenticate period** { *time* | **default** }	配置重认证定时器时间，整数形式，取值范围为 60～3600，单位为秒，默认值为 60。
4	JX(config-ge-1/0/*)#**dot1x timer quiet-period** { *time* | **default** }	配置静默定时器时间，整数形式，取值范围为 10～3600，单位为秒，默认值为 60。
5	JX(config-ge-1/0/*)#**dot1x supp period** *time*	配置 Request/MD5 Challenge 请求报文超时定时器，整数形式，取值范围为 6～60，单位为秒，默认值为 5。
6	JX(config-ge-1/0/*)#**dot1x server-timeout period** { *time* | **default** }	配置认证服务器超时定时器时间，整数形式，取值范围为 60～600，单位为秒，默认值为 120。
7	JX(config-ge-1/0/*)#**dot1x tx period** { *time* | **default** }	配置 Request/Identity 请求报文超时定时器，整数形式，取值范围为 30～60，单位为秒，默认值为 30。

8.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show dot1x config**	查看所有 802.1x 相关配置信息。
2	JX#**show dot1x information**	查看 802.1x 协议统计信息。
3	JX#**show dot1x user**	查看 802.1x 协议认证的用户信息。
4	JX#**show dot1x** *interface-type interface-number*	查看接口下 802.1x 相关统计及配置信息。

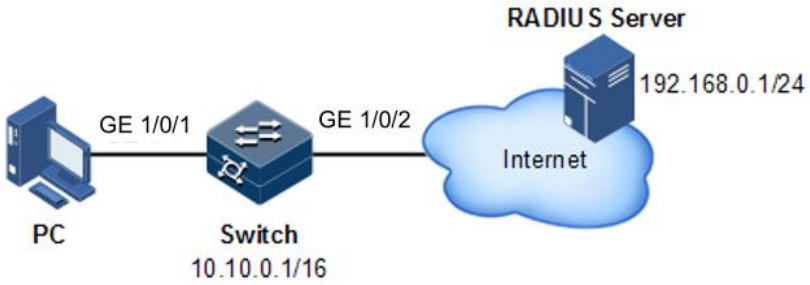
8.3.8 配置 802.1x 示例

组网需求

为了使用户访问外部网络，如下图所示，在交换机上配置 802.1x 认证，具体要求如下：

- 交换机的 IP 地址是 10.10.0.1，掩码是 255.255.0.0，缺省网关地址为 10.10.0.2。
- 通过 RADIUS 服务器进行认证和授权，RADIUS 服务器的 IP 地址是 192.168.0.1，密码是 JX。
- 在认证通过后，可以在 600s 后自动发起重认证过程。

图 8-4 802.1x 应用组网示意图



配置步骤

步骤 1 配置交换机 IP 地址及 RADIUS 服务器地址。

```
JX#config
JX(config)#interface vlan 1
JX(config-vlan1)#ip address 10.10.0.1/16
JX(config-vlan1)#exit
JX(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
JX(config)#exit
JX(config)#aaa
JX(config-aaa)#radius-server host server1 ip-address 192.168.0.1 key
12345
JX(config-aaa)#server-group grp1 radius-server server1
JX(config-aaa)#aaa authentication dot1x method d1 first grp1
```

步骤 2 使能全局及接口 802.1x 认证功能。

```
JX#config
JX(config)#dot1x start
JX(config)#dot1x aaa authentication method d1
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dot1x enable
JX(config-ge-1/0/1)#dot1x reauthenticate period 600
```

检查结果

通过 **show dot1x** 命令查看设备上 802.1x 功能的配置结果。

```
JX#show dot1x interface ge 1/0/1
Interface ge 1/0/1 dot1x information:
-------------------------------------------------------------
```

```
Authentication Guest Vlan    : n/a
Max User Num               : 128
Default Max User Num        : 128
Current User Num           : 0
Authen Success User Num     : 0
Authen Fail User Num        : 0
Authen Timeout User Num     : 0
Authenting User Num         : 0
Authentication Method       : Method4
Accounting Method           : Method5
Quiet                      : Disable
Reauthentication            : Enable
Reauthentication Period     : 600
Mac Bypass                 : Disable
Offline Detect             : Disable
Restrict Vlan              : n/a
Critical Vlan              : n/a
TX Period                  : 30
Supp Timeout Period         : 5
Server time Period          : 120
Port Control               : Auto
Port Method                : Mac Based
Port Auth State            : Unauthenticated
Auth Method                : Chap
Not Eapol Trigger           : Disable
Trigger Authen Type         : None
Trigger Auth Pkt Type       : ARP NDP DHCP DHCP6
Rx Eapol Start Pkt Num      : 0
Rx Eapol Logoff Pkt Num     : 0
Rx Eap Idenitity Pkt Num    : 0
Rx Eap MD5 Pkt Num          : 0
Tx Eap Success Pkt Num      : 0
Tx Eap Fail Pkt Num         : 0
Tx Eap Idenitity Pkt Num    : 0
Tx Eap MD5 Pkt Num          : 0
-------------------------------------------------------------
```

8.4 安全 MAC

8.4.1 简介

接口安全 MAC 主要应用于网络边缘用户侧的交换设备上，用于保证某个接口接入数据的安全性，根据源 MAC 地址对输入的报文加以控制。用户可以启动接口安全功能来限制和区分哪些用户可以通过安全接口来访问网络，只有接口安全 MAC 地址才能够访问网络，非安全 MAC 地址均按照用户配置的接口访问违例模式处理。

安全 MAC 地址分类

设备支持的安全 MAC 地址分为以下两类：

- 安全 MAC 地址

动态安全 MAC 地址是由设备自己学习得到的。用户可以在允许学习的 MAC 地址最大数目范围内，将学习到的 MAC 地址都设置为安全 MAC 地址。该类安全 MAC 地址不会被老化，但是不支持配置加载。

- Sticky 安全 MAC 地址

Sticky 安全 MAC 地址由用户在安全接口手动配置生成或者由安全 MAC 地址转化而来。与安全 MAC 地址不同，Sticky 安全 MAC 地址需要配合 Sticky 学习功能一起使用，支持配置加载：

说明

- 当 Sticky 学习功能使能时，接口下学习到的所有安全 MAC 地址均转换为 Sticky 安全 MAC 地址。
- 当 Sticky 学习功能禁止时，接口下所有 Sticky 安全 MAC 地址均转换为安全 MAC 地址。

安全 MAC 违例处理方式

当接口安全 MAC 的数目已经达到最大数目时，再有陌生源 MAC 报文输入则视为违规操作。对于非法的用户接入，根据安全 MAC 的违规策略配置交换机的不同处理方式如下：

- Protect 模式：对于非法接入的用户，安全接口直接丢弃该用户的报文。
- Restrict 模式：对于非法接入的用户，安全接口丢弃该用户的报文，同时在控制台打印 Syslog 信息，并发送告警信息至网管系统。
- Shutdown 模式：对于非法接入的用户，安全接口丢弃该用户的报文，同时在控制台打印 Syslog 信息、发送告警信息至网管系统并将该安全接口关闭。

注意

当发生 MAC 地址飘移，即安全接口 A 收到一个已经存在于安全接口 B 中的安全 MAC 所对应用户的访问时，安全接口 A 将其作为违例处理。

8.4.2 配置准备

场景

为了保证交换机接口接入数据的安全性，可以根据源 MAC 地址对输入的报文加以控制。通过安全 MAC 可以将接入接口配置成只允许特定的几个用户接入，也可以配置成允许特定数量的用户从该接口接入。但接入的用户超过限制时，接入的报文将按照安全 MAC 的违规策略进行处理。

前提

无

8.4.3 安全 MAC 功能的缺省配置

设备上安全 MAC 功能的缺省配置如下。

功能	缺省值
接口安全 MAC 功能状态	禁止
动态安全 MAC Sticky 学习功能状态	禁止
接口安全 MAC Trap 功能状态	禁止
接口安全 MAC 违规处理方式	**restrict**
接口安全 MAC 的最大数量	1024

8.4.4 配置安全 MAC 基本功能

注意

- 不建议用户在聚合组的单个成员接口上使能接口安全 MAC 功能。
- 不建议用户在同一接口上使能接口安全 MAC 功能的同时，使用 MAC 地址管理功能来配置静态 MAC 地址，会导致接口安全 MAC 功能失效。
- 当 802.1x 接口认证方式为基于 MAC 地址进行认证时，安全 MAC 功能与 802.1x 功能互斥，不建议用户在同一接口上同时进行配置。
- 安全 MAC 功能与基于接口和基于接口 VLAN 的 MAC 地址数目限制互斥，不能同时配置。

请在设备上进行以下配置。

步骤	配置	说明
1	JX**#config**	进入全局配置模式。
2	JX(config)**#interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/1)**#port-security enable**	使能接口安全 MAC 功能。
4	JX(config-ge-1/0/1)**#port-security maximum** { *maximum* | **default** }	配置接口安全 MAC 最大数目，整数形式，取值范围为 1～1024，默认值为 1。
5	JX(config-ge-1/0/1)#port-security protect-action { **protect** | **restrict** | **shutdown** }	配置安全 MAC 违例模式。
6	JX(config-ge-1/0/1)**#shutdown** JX(config-ge-1/0/1)**#no shutdown**	将因违反接口安全 MAC 而被关闭的接口重新开启。

步骤	配置	说明
7	JX(config)# **port-security error-down recovery-interval** { *second* | **default** }	(可选)配置接口安全 MAC 恢复时间，整数形式，单位为秒，取值范围为 3～86400，默认值为 0 秒。

说明

当安全 MAC 违规策略为 Shutdown 模式时，可以使用该命令将因违反接口安全 MAC 而被关闭的接口重新开启。

当接口 Up 以后，配置的安全 MAC 违例模式继续保持。

8.4.5 配置接口 Sticky 安全 MAC 地址

注意

建议用户不要在 Sticky 安全 MAC 功能禁止的情况下配置 Sticky 安全 MAC 地址，否则可能导致功能异常。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/1)#**port-security enable**	使能接口安全 MAC 功能。
4	JX(config-ge-1/0/1)#**port-security mac-address sticky enable**	使能 Sticky 安全 MAC 学习功能。
5	JX(config-ge-1/0/1)#**port-security mac-address sticky vlan** *vlan-id* **mac** *mac-address*	手动配置接口 Sticky 安全 MAC 地址。

说明

Sticky 安全 MAC 学习功能使能后，动态安全 MAC 地址转换为 Sticky 安全 MAC 地址；手动设置的 Sticky 安全 MAC 地址生效。

8.4.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show mac-address config**	查看安全 MAC 的配置信息。
2	JX#**show mac-address { security | sticky }**	查看安全 MAC 地址表项信息。

8.4.7 维护

用户可以通过以下命令，维护设备安全 MAC 特性的运行情况和配置情况。

命令	描述
JX(config)#**no mac-address** { **security** | **sticky** } [*interface-type interface-number*]	清除指定类型的安全 MAC。

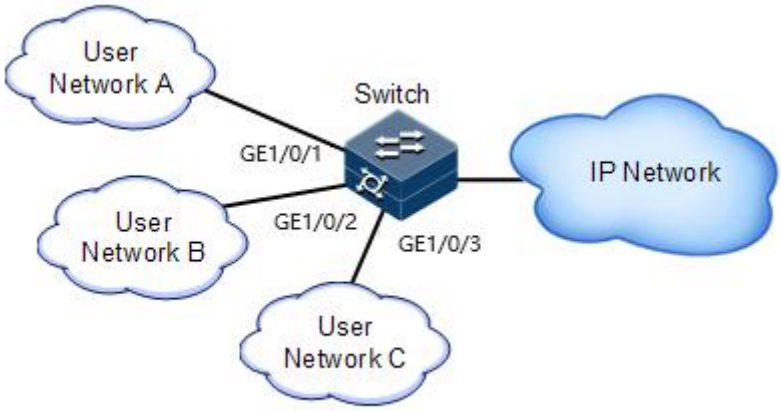
8.4.8 配置安全 MAC 示例

组网需求

如下图所示，交换机下联 3 个用户网络，为了保证交换机接口接入数据的安全性，要求配置如下：

- 接口 GE 1/0/1 最大允许 3 个用户接入网络。其中一个指定用户的 MAC 地址为 0000.0000.0001。其他 2 个用户为动态学习。违例模式采用 Protect 模式
- 接口 GE 1/0/2 最大允许 2 个用户接入网络。这 2 个用户的 MAC 地址通过学习确定。违例模式采用 Restrict 模式。
- 接口 GE 1/0/3 要求最大允许 1 个用户接入网络。该指定用户的 MAC 地址为 0000.0000.0002，违例模式采用 Shutdown 模式。

图 8-5 安全 MAC 应用组网示意图



配置步骤

步骤 1 配置 GE 1/0/1 接口安全 MAC。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port-security enable
JX(config-ge-1/0/1)#port-security maximum 3
JX(config-ge-1/0/1)#port-security mac-address sticky enable
JX(config-ge-1/0/1)#port-security mac-address sticky vlan 1
mac 00:00:00:00:00:01
JX(config-ge-1/0/1)#quit
```

步骤 2 配置 GE 1/0/2 的接口安全 MAC。

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port-security enable
JX(config-ge-1/0/2)#port-security maximum 2
JX(config-ge-1/0/2)#port-security protect-action restrict
JX(config-ge-1/0/2)#quit
```

步骤 3 配置 GE 1/0/3 的接口安全 MAC。

```
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port-security enable
JX(config-ge-1/0/3)#port-security maximum 1
JX(config-ge-1/0/3)#port-security protect-action shutdown
JX(config-ge-1/0/3)#port-security mac-address sticky enable
JX(config-ge-1/0/3)#port-security mac-address sticky vlan 1
mac 00:00:00:00:00:02
JX(config-ge-1/0/3)#quit
```

检查结果

通过 **show mac-address config** 查看安全 MAC 的接口配置是否正确。

```
JX#show mac-address config
!
```

```
mac-address aging-time 500
!
interface ge 1/0/1
 port-security enable
 port-security maximum 3
 port-security mac-address sticky enable
!
interface ge 1/0/2
 port-security enable
 port-security maximum 2
!
interface ge 1/0/3
 port-security enable
 port-security protect-action shutdown
 port-security mac-address sticky enable
```

通过 **show mac-address sticky** 查看设备上接口安全 MAC 地址配置及学习情况。

```
JX(config)#show mac-address sticky
  MacAddress         VLAN/VSI/BD Learned-From    Type       Valid
------------------------------------------------------------------------
  0000:0000:0001     1/--/--     ge-1/0/1        sticky     yes
  0000:0000:0002     1/--/--     ge-1/0/3        sticky     yes
------------------------------------------------------------------------
  Total:2
```

8.5 PPPoE+

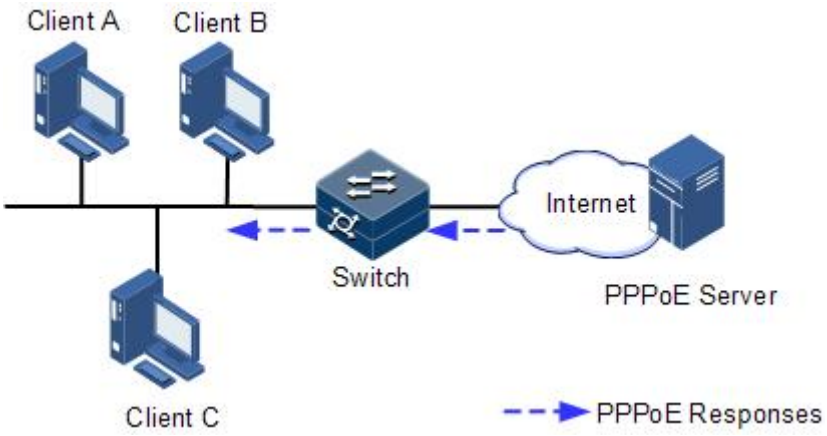
8.5.1 简介

PPPoE+（PPPoE Intermediate Agent，PPPoE 中继代理）协议用于对 PPPoE（Point to Point Protocol Over Ethernet，基于以太网承载点到点协议）认证报文进行处理，即对 PPPoE 报文附加更多接入设备信息，使服务器能获得足够的信息辨别用户。PPPoE+协议可以有效防止在 PPPoE 认证过程中的账号共享或者账号盗用问题，保证了网络的安全性。

使用 PPPoE 拨号方式连接网络，用户通过设备的不同接口，只要通过同一个认证服务器认证成功，就可以使用这个账号访问网络。但是服务器仅根据包含用户名和密码的认证信息，很难对用户进行区分。增加 PPPoE+特性以后，认证时除了需要用户名和密码信息外，在认证报文中还将携带设备接口等信息。如果认证服务器识别的接口号等信息与配置不一致，则认证不通过，这样就可以防止非法用户盗用其他合法用户的账号进行上网。

PPPoE 协议采用客户端/服务器模式，如下图所示，Switch 起到中继代理的作用，用户通过 PPPoE 认证连接网络。如果服务器需要定位用户，在认证报文中则需要更多的客户信息。

图 8-6 用户通过 PPPoE 认证连接网络示意图



用户通过 PPPoE 访问网络需要经过两个阶段：第一个阶段是发现阶段，即认证阶段，第二个阶段是会话阶段。PPPoE+功能需要处理的就是发现阶段的报文。

- 客户端通过 PPPoE 访问网络，首先会发送一个广播报文 PADI（PPPoE Active Discovery Initiation，PPPoE 活动发现发起报文），该报文的作用是查找认证服务器；
- 收到 PADI 报文的认证服务器会发送一个单播 PADO（PPPoE Active Discovery Offer，PPPoE 活动发现提供报文）报文响应；
- 如果有多个认证服务器发送了 PADO 报文，客户端会从中选择一个，发送单播 PADR（PPPoE Active Discovery Request，PPPoE 活动发现请求报文）报文请求认证；
- 认证服务器收到 PADR 报文后，如果判定用户合法，则发送一个单播报文 PADS（PPPoE Active Discovery Session-confirmation，PPPoE 活动发现会话确认报文）作为 PADR 的响应。至此，发现阶段完毕。

PPPoE+的主要功能是在 PADI 和 PADR 报文中添加用户标识信息，服务器可以判定标识信息是否和用户账号匹配，决定是否分配资源。

8.5.2 配置准备

场景

为了防止在 PPPoE 认证过程中有非法用户接入，需要配置 PPPoE+功能，在 PPPoE 协议报文中加入附加的用户标识信息。

由于添加的用户标识信息和具体的交换机及接口相关，因此认证服务器可以将用户和交换机以及接口等信息绑定。从而有效防止账号共享和账号盗用问题，还可以更好的定位用户，以保证网络的安全性。

前提

无

8.5.3 PPPoE+功能的缺省配置

设备上 PPPoE+功能的缺省配置如下。

功能	缺省值
全局 PPPoE+功能状态	禁止
接口 PPPoE+功能状态	禁止
全局 PPPoE+Tag 的收包处理策略	replace
Circuit ID 的填充模式	SwitchCommon 模式
Circuit ID 信息	接口名/外层 VLAN 号/内层 VLAN 号
Circuit ID 的附加字符串	无
Remote ID 填充的 MAC 地址	交换机的 MAC 地址
Remote ID 填充形式	二进制形式
接口信任状态	非信任接口
PPPoE+ Tag 收包处理策略	替换

说明

缺省情况下，PPPoE 报文可以通过接口并且不会被附加任何信息。

8.5.4 配置 PPPoE+基本功能

注意

PPPoE+功能用于处理 PADI 和 PADR 报文，只针对 PPPoE 的客户端。一般只有连接客户端的接口使能 PPPoE+功能，而信任接口是指交换机与 PPPoE 服务器连接的接口，这两种接口角色是互斥的，即一个接口不能既使能 PPPoE+功能又是信任接口。

使能 PPPoE+功能

使能设备全局和接口的 PPPoE+功能后，发送到该接口的 PPPoE 认证报文会附加上用户信息，再发往信任接口。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**pppoeplus start**	使能全局 PPPoE+功能。
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	JX(config-ge-1/0/1)#**pppoeplus enable**	使能接口 PPPoE+功能。

配置 PPPoE+信任接口

配置 PPPoE+信任接口主要是为了降低 CPU 使用率，信任接口收到的 PPPoE 报文不会上送 CPU 处理，由交换芯片直接转发。通常配置在与 PPPoE 服务器相连的接口上。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/1)#**pppoeplus trust**	配置 PPPoE+的信任接口。

8.5.5 配置 PPPoE+报文信息

PPPoE+功能主要是对 PPPoE 报文中的一个特定 Tag 进行处理，这个 Tag 包含 Circuit ID 和 Remote ID 两个字段。其中：

- Circuit ID 填充的是接收客户端请求报文接口的接口名、所属于的 VLAN ID（包括外层 VLAN ID 和内层 VLAN ID）
- Remote ID 填充的是接收客户端请求报文接口的 MAC 地址或者交换机的 MAC 地址。

配置 Circuit ID

Circuit ID 有三种填充模式：ascii 模式、default 模式和 user-define 模式。

各 Circuit ID 填充模式意义如下：

- ascii：即 Circuit ID 填充为命令行配置的字符串。
- default：即 Circuit ID 为默认值。
- user-define：即按照用户自定义格式填充 Circuit ID。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**pppoeplus default circuit-id format** { **ascii** | **default** | **user-define** } *string*	配置交换机 Circuit ID。（default 模式不需要再配置字符串）
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	JX(config-ge-1/0/1)#**pppoeplus circuit-id format** { **ascii** | **default** | **user-define** } *string*	在接口上配置 Circuit ID。 （default 模式不需要再配置字符串，如果接口和全局都配置了 circuit-id，则接口的配置优先生效）

配置 Remote ID

Remote ID 有三种填充模式：ascii 模式、default 模式和 user-define 模式。

各 Remote ID 填充模式意义如下：

- ascii：即 Circuit ID 填充为命令行配置的字符串。
- default：即 Circuit ID 为默认值。
- user-define：即按照用户自定义格式填充 Circuit ID。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**pppoeplus default remote-id format** { **ascii** | **default** | **user-define** } *string*	配置交换机 Remote ID。（default 模式不需要再配置字符串）
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	JX(config-ge-1/0/1)#**pppoeplus remote-id format** { **ascii** | **default** | **user-define** *string* }	在接口上配置 Remote ID。 （default 模式不需要再配置字符串，如果接口和全局都配置了 remote-id，则接口的配置优先生效）

配置 PPPoE+Tag 处理策略

由于某些原因，如某些信息字段的 Tag 可能是客户端伪造的，需要将报文原有的 Tag 替换掉。配置 PPPoE+Tag 收包处理策略为替换后，如果 PPPoE 报文已经携带信息字段 Tag，会将其替换；如果配置 PPPoE+Tag 收包处理策略为保持，则如果 PPPoE 报文已

经携带信息字段 Tag，就保留原 tag；如果配置 PPPoE+Tag 收包处理策略为丢弃，则如果 PPPoE 报文已经携带信息字段 Tag，就会丢弃原 tag。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**pppoeplus default policy** { **drop** | **keep** | **replace** }	配置全局的 PPPoE+Tag 的收包处理策略。
	JX(config-ge-1/0/1)# **pppoeplus policy** { **drop** | **keep** | **replace** }	配置接口上的 PPPoE+Tag 的收包处理策略。如果接口和全局都配置了收包处理策略，则接口的配置优先生效

8.5.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show pppoeplus config**	查看 PPPoE+的配置信息。
2	JX#**show pppoeplus information**	查看 PPPoE+模块当前的全局配置信息，包括默认配置信息。

8.5.7 维护

用户可以通过以下命令，维护 PPPoE+特性的运行情况和配置情况。

命令	描述
JX(config)#**reset pppoeplus statistic** [**interface** *interface-type interface-number*]	清除 PPPoE+的统计信息，支持指定端口清除统计信息。
JX#**show pppoeplus interface** [*interface-type interface-number*]	查看 PPPoE+的接口上的配置和统计信息。

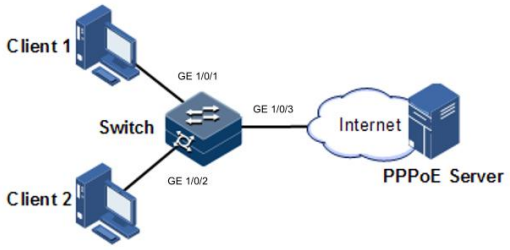
8.5.8 配置 PPPoE+示例

组网需求

如下图所示，为了防止在 PPPoE 认证过程中非法用户的接入，对用户上网进行控制和监管，可以在交换机上配置 PPPoE+功能，具体要求如下：

- 接口 GE 1/0/1 和 GE 1/0/2 分别连接 Client 1 和 Client 2，GE 1/0/3 连接 PPPoE 服务器；
- 使能全局 PPPoE+功能和 GE 1/0/1、GE 1/0/2、GE 1/0/3 的 PPPoE+功能，配置 GE 1/0/3 为信任接口；
- 配置 Circuit ID 类型为用户自定义，格式为接口名加外层 VLAN ID 加设备名；配置 Remote ID 类型为 ascii，内容为 01:02:03:04:05:06；
- 配置接口 GE 1/0/1 和 GE 1/0/2 的 PPPoE+Tag 的收包处理策略。

图 8-7 PPPoE+应用组网示意图



配置步骤

步骤 1 使能全局 PPPoE+功能，并使能 GE 1/0/1、GE 1/0/2 和 GE 1/0/3 的 PPPoE+功能。

```
JX(config)#pppoeplus start
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#pppoeplus enable
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#pppoeplus enable
JX(config-ge-1/0/2)#exit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#pppoeplus enable
JX(config-ge-1/0/3)#exit
```

步骤 2 配置 GE 1/0/3 为信任接口。

```
JX#config
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#pppoeplus trust
JX(config-ge-1/0/3)#exit
```

步骤 3 配置 circuit-id 和 remote-id 的格式。

```
JX(config)#pppoeplus default circuit-id format user-
defined %portname:%svlan:%devicename
JX(config)#pppoeplus default remote-id format ascii 01:02:03:04:05:06
```

步骤 4 配置 GE 1/0/1 和 GE 1/0/2 的 PPPoE+Tag 的收包处理策略。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#pppoeplus policy keep
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#pppoeplus policy drop
```

```
JX(config-ge-1/0/2)#exit
```

检查结果

通过 **show pppoeplus config** 命令查看设备上 PPPoE+功能的配置结果。

```
JX#show pppoeplus config
!
pppoeplus start
pppoeplus default remote-id format ascii 01:02:03:04:05:06
pppoeplus default circuit-id format user-
defined %portname:%svlan:%devicename
!
interface ge 1/0/1
 pppoeplus enable
 pppoeplus policy keep
!
interface ge 1/0/2
 pppoeplus enable
 pppoeplus policy drop
!
interface ge 1/0/3
 pppoeplus enable
 pppoeplus trust
```

8.6 风暴抑制

8.6.1 简介

二层网络是一个广播域，当接口接收到大量的广播、未知组播和未知单播报文时，就会产生广播风暴。如果不对广播风暴进行限制，就会耗费大量的网络带宽，造成网络速率下降，甚至造成通信中断，影响正常报文的转发。

风暴抑制与风暴控制能对网络中的广播流量进行限制，能在广播流量激增时抑制广播风暴的产生，从而保证正常报文的转发。

广播风暴产生

下面几种情况可能会产生广播风暴：

- 未知单播报文：目的 MAC 地址不在 MAC 地址表中的单播报文，即 DLF（Destination Lookup Failure，寻找目标失败）报文，如果某段时间内此种报文流量过多，进行大量的广播发送，可能会形成广播风暴。
- 未知组播报文：目的 MAC 地址不在 MAC 地址表中的组播报文，如果某段时间内此种报文流量过多，进行大量的广播发送，可能会形成广播风暴。
- 广播报文：目的 MAC 地址为广播的报文，如果某段时间内此种报文流量过多，可能会形成广播风暴。

风暴抑制原理

风暴抑制是对网络上可能形成广播风暴的广播、未知组播或未知单播报文进行过滤。当设备接收到的广播报文超过一定阈值时，将进行相应的动作。

风暴抑制方式

方式有以下几种：

- BPS（Bits Per Second，每秒位数）：每秒允许通过的位数。
- PPS（Packets Per Second，每秒包数）：每秒允许通过的包数。
- Percent：以接口最大速率的百分比进行限速，仅物理口支持

8.6.2 配置准备

场景

在二层网络中配置风暴抑制功能，当网络中未知组播、未知单播和广播报文增多时可以抑制广播风暴的产生，从而保证正常报文的转发。

前提

无

8.6.3 风暴抑制的缺省配置

设备上风暴抑制的缺省配置如下。

功能	缺省值
广播流量风暴抑制状态	禁用
未知单播流量的风暴抑制状态	禁用
未知组播流量的风暴抑制状态	禁用
接口的风暴抑制动作	无
接口的恢复周期	30s
接口风暴抑制 Trap 功能	禁用

8.6.4 配置风暴抑制功能

注意

风暴抑制和基于 VLAN 的流量限速功能会相互影响，不建议用户在同一接口上同时开启这两个功能。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口节点。
3	JX(config-ge-1/0/1)#**storm-suppression { unknown-unicast | unknown-multicast | broadcast } min-rate { kbps | mbps }** *rate-value* **max-rate { kbps | mbps }** *rate-value*	使能接口下的风暴抑制功能，使用 BPS 配置风暴抑制的限速阈值。
	JX(config-port-channel*)#**storm-suppression { unknown-unicast|unknown-multicast|broadcast } min-rate percent** *rate-value* **max-rate percent** *rate-value*	使能接口下的风暴抑制功能，使用比例配置风暴抑制的限速阈值。
4	JX(config-ge-1/0/1)#**storm-suppression action { block | error-down | none }**	配置接口的风暴抑制动作。
5	JX(config-ge-1/0/1)#**storm-suppression interval {** *interval* **| default }**	配置风暴抑制关闭接口后接口的恢复周期。
6	JX(config-ge-1/0/1)#**storm-suppression snmp-trap enable**	使能接口风暴抑制 Trap 功能，使用 disable 模式禁用接口风暴抑制 trap 功能。
7	JX(config-ge-1/0/1)#**exit**	返回全局配置模式。

8.6.5 检查风暴抑制配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show storm-suppression interface** [*interface-type interface-number*]	查看风暴抑制接口配置信息。
2	JX#**show storm-suppression information**	查看风暴抑制全局配置信息。

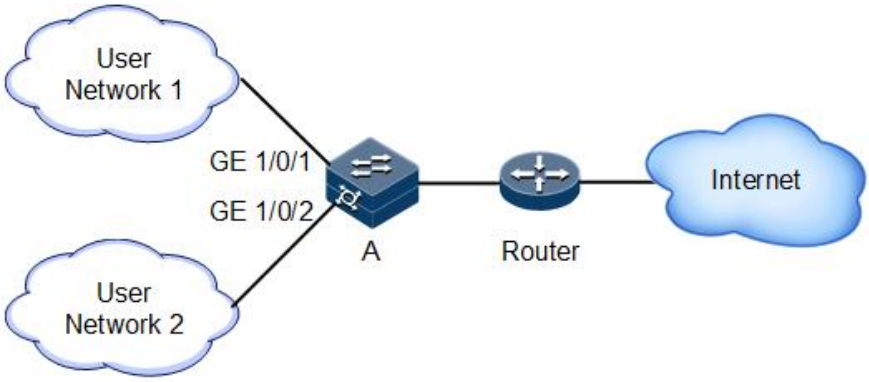
8.6.6 配置风暴抑制应用示例

组网需求

如下图所示，当 Switch A 的 GE 1/0/1 和 GE 1/0/2 接口接收到大量的未知单播或广播报文，Switch A 就会向 VLAN 内除了接收接口之外的所有接口转发这些报文，就可能会导致广播风暴，降低 Switch A 的转发性能。

为限制广播风暴对 Switch A 的影响，需要在 Switch A 的 GE 1/0/1 和 GE 1/0/2 接口上部署风暴抑制功能，分别限制来自用户网络 1 和用户网络 2 的广播报文，抑制阈值为 640kbit/s，若超限，则执行 shutdown 操作，低于 320kbit/s 才打开端口。

图 8-8 风暴抑制应用组网示意图



配置步骤

步骤 1 配置风暴抑制阈值。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#storm-suppression broadcast min-rate kbps 320 max-
rate kbps 640
JX(config-ge-1/0/1)#storm-suppression action error-down
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#storm-suppression broadcast min-rate kbps 320 max-
rate kbps 640
JX(config-ge-1/0/2)#storm-suppression action error-down
```

检查结果

通过 **show storm-suppression interface** 查看风暴抑制配置是否正确。

```
JX(config-ge-1/0/2)#show storm-suppression interface
NOTE :
  UNMC: unknown multicast ; BC: broadcast ; UNC: unknown unicast
 Interface     Type    State   RateMode  Min/MaxRate          Action/Status
Interval
------------------------------------------------------------------------
----------------------
 ge-1/0/1      UNC     disable bps      n/a                  none/normal
5
               UNMC    disable bps      n/a                  none/normal
5
               BC      enable  bps      320/640 (kbit/s)      none/errordown
5
 ge-1/0/2      UNC     disable bps      n/a                  none/normal
5
```

```
                UNMC    disable bps      n/a                  none/normal
5
                BC      enable  bps      320/640 (kbit/s)      none/errordown
5
------------------------------------------------------------------------------
----------------------
```

8.7 ARP 防攻击

8.7.1 配置准备

场景

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。

攻击者可以仿冒用户、仿冒网关发送伪造的 ARP 报文，使网关或主机的 ARP 表被篡改。如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下 ARP 防攻击功能。

前提

无

8.7.2 ARP 防攻击缺省配置

缺省没有配置任何 ARP 防攻击配置

8.7.3 配置 ARP 防攻击功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**arp-antiattack src-ip enable**	针对 ARP 源 IP 地址的 ARP 冲突检测。通过 ARP 报文中的源 IP 地址，查找 ARP 表，如果找到了对应的 ARP 表项，并且 ARP 表项中对应的 MAC 地址和 ARP 报文中的源 MAC 地址不一致，则认为是 ARP 冲突。会丢弃该 ARP 报文，防止攻击者篡改 ARP 表中的 MAC 地址。

步骤	配置	说明
3	JX(config)#**arp-antiattack src-mac enable**	针对 ARP 源 MAC 地址的 ARP 冲突检测。通过 ARP 报文中的源 MAC 地址，查找 ARP 表，如果找到了对应的 ARP 表项，并且 ARP 表项中对应的 IP 地址和 ARP 报文中的源 IP 地址不一致，则认为是 ARP 冲突。会丢弃该 ARP 报文，防止攻击者篡改 ARP 表中的 IP 地址。
4	JX(config)#**arp-antiattack arp-cheat enable**	仿冒本设备的 ARP 欺骗检测。检测设备收到 ARP 报文里的源或者目的 IP 地址，以及源 MAC 地址和 ARP 报文类型，判断 ARP 报文是否是仿冒本设备的攻击包，如果判断为攻击包，则会丢弃该 ARP 报文，并发送一个本设备的免费 ARP。
5	JX(config)#**arp-antiattack gratuitous-arp enable**	免费 ARP 报文主动丢弃。使能免费 ARP 报文主动丢弃功能后，设备直接丢弃免费 ARP 报文，可以防止设备因处理大量免费 ARP 报文，导致 CPU 负荷过重而无法处理其他业务。
6	JX(config)#**arp-antiattack gateway-cheat enable**	ARP 防网关冲突。通过 ARP 防网关冲突功能，可以防止用户仿冒网关发送 ARP 报文，非法修改网络内其他用户的 ARP 表项。ARP 防网关冲突和动态 ARP 检测不能同时配置。
7	JX(config-ge-*/*/*)# **arp-antiattack check user-bind enable**	动态 ARP 检测，即 DAI(Dynamic ARP Inspection)。使能动态 ARP 检测的检测项，三个检查项可自由组合。默认是三个检查项都检查 DAI(Dynamic ARP Inspection)功能后，当设备收到 ARP 报文时，将此 ARP 报文的源 IP、源 MAC、收到 ARP 报文的接口及 VLAN 信息和 DHCP Snooping 绑定表的信息进行比较，如果信息匹配，则认为是合法用户，允许此用户的 ARP 报文通过，否则认为是攻击，丢弃该 ARP 报文。本功能仅适用于 DHCP Snooping 场景。
8	JX(config-ge-1/0/1)#**arp-antiattack check user-bind check-item { vlan | ip-address | mac-address }**	动态 ARP 检测的检测项，三个检查项可自由组合。默认是三个检查项都检查。

8.7.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show arp-antiattack config	查看 ARP 防攻击配置信息。
2	JX#show arp-antiattack interface	查看动态 ARP 检测项。
3	JX#show arp-antiattack information	查看 ARP 防攻击全局信息

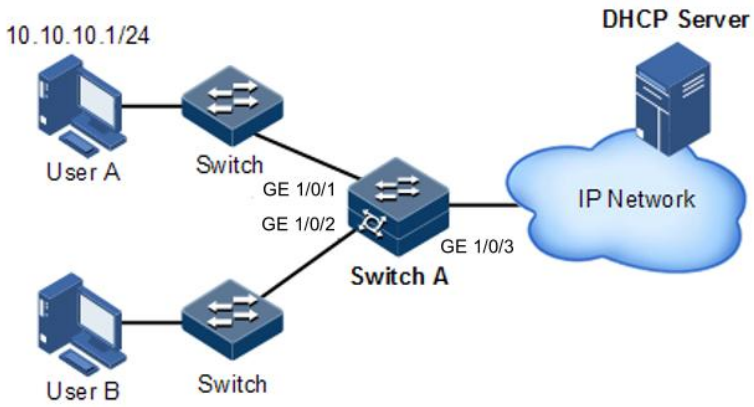
8.7.5 配置 ARP 防攻击示例

组网需求

为了防止 ARP 攻击，如下图所示，需要在 Switch A 设备上配置 ARP 防攻击功能。要求如下：

- 免费 ARP 报文不允许通过，使能针对 ARP 源 IP 地址和源 mac 地址的 ARP 冲突检测，以及仿冒本设备的 ARP 欺骗检测功能。
- Switch A 作为 User A 的网关，使能 ARP 防网关冲突。
- 清除 Switch A 上的 ARP 防网关冲突配置，Switch A 提供 User B 到 DHCP Server 的二层可达性，在 GE 1/0/2 上配置动态 ARP 检测功能。1

图 8-9 动态 ARP 检测应用组网示意图



配置步骤

步骤 1 配置针对 ARP 源 IP 地址的 ARP 冲突检测。

```
JX#config
JX(config)#arp-antiattack src-ip enable
```

步骤 2 配置针对 ARP 源 MAC 地址的 ARP 冲突检测。

```
JX(config)# arp-antiattack src-mac enable
```

步骤 3 使能仿冒本设备的 ARP 欺骗功能。

```
JX(config)#arp-antiattack arp-cheat enable
```

步骤 4 使能免费 ARP 报文主动丢弃。

```
JX(config)#arp-antiattack gratuitous-arp enable
```

步骤 5 使能 ARP 防网关冲突。

```
JX(config)#arp-antiattack gateway-cheat enable
```

步骤 6 使能动态 ARP 检测，要先去使能 ARP 防网关冲突。

```
JX(config)#arp-antiattack gateway-cheat disable
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#arp-antiattack check user-bind enable
JX(config-ge-1/0/2)#exit
JX(config)#
```

检查结果

通过 **show arp-antiattack config** 命令查看设备上 ARP 防攻击的配置。

```
JX#show arp-antiattack config
Version: ANTIARP_VL2.10.00.00
!
arp-antiattack src-ip enable
arp-antiattack src-mac enable
arp-antiattack arp-cheat enable
arp-antiattack gratuitous-arp enable
arp-antiattack gateway-cheat enable

JX#show arp-antiattack config
Version: ANTIARP_VL2.10.00.00
!
arp-antiattack src-ip enable
arp-antiattack src-mac enable
arp-antiattack arp-cheat enable
arp-antiattack gratuitous-arp enable
!
interface ge 1/0/2
 arp-antiattack check user-bind enable
```

8.8 ND Snooping

8.8.1 简介

ND（Neighbor Discovery，邻居发现）是确定邻居节点之间关系的一组消息和进程。邻居发现协议替代了 IPv4 的 ARP（Address Resolution Protocol）、ICMP 路由器发现（Router Discovery）和 ICMP 重定向（Redirect）消息，并提供了地址冲突检测、邻居地址解析、确定邻居可达性以及进行主机地址配置等功能。

ND Snooping 功能主要应用于接入设备上，检查用户的合法性。对于合法用户的 ND 报文进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

用户合法性检查是根据 ND 报文中源 IPv6 地址和源 MAC 地址，检查用户是否是报文收到端口所属 VLAN 上的合法用户。

ND Snooping 功能将接入设备上的端口分为两种：ND 信任端口、ND 非信任端口。

- 对于 ND 信任端口：不进行用户合法性检查。从 ND 信任端口接收到的 ND 报文，设备可以进行正常转发。
- 对于 ND 非信任端口：从 ND 非信任端口接收到的 RA 报文，设备会认为是非法报文直接丢弃；从 ND 非信任端口接收到的 NA/RS/NS 报文，则会通过 ND 报文合法性检查功能进行绑定表匹配检查，当不符合绑定表关系时，设备会认为是非法报文直接丢弃；从 ND 非信任端口接收到的其他类型报文，设备进行正常转发。

8.8.2 配置准备

场景

ND Snooping 用来防止网络中常见的 ND 欺骗攻击，实现了对不安全来源的 ND 报文进行隔离。是否对 ND 报文信任通过配置接口的信任状态实现，而是否符合要求则通过配置绑定表实现。

前提

无

8.8.3 ND Snooping 的缺省配置

设备上 ND Snooping 的缺省配置如下。

功能	缺省值
ND Snooping 接口信任状态	不信任
全局 ND Snooping 功能	未启动
端口 ND Snooping 功能	未使能
NS、NA、RS 报文检查功能	未使能

8.8.4 配置 ND Snooping

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**nd-snooping start**	开启全局 ND Snooping 功能。

步骤	配置	说明
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口或 VLAN 接口配置模式。
4	JX(config-ge-1/0/*)#**nd-snooping enable**	配置连接网关的接口开启 ND Snooping 功能。
5	JX(config-ge-1/0/*)#**nd-snooping trust**	配置连接网关的接口为信任接口。
6	JX(config)#**nd-snooping check { na | ns | rs } enable**	开启 ND Snooping 对 ns、na、rs 报文的合法性检查。

8.8.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

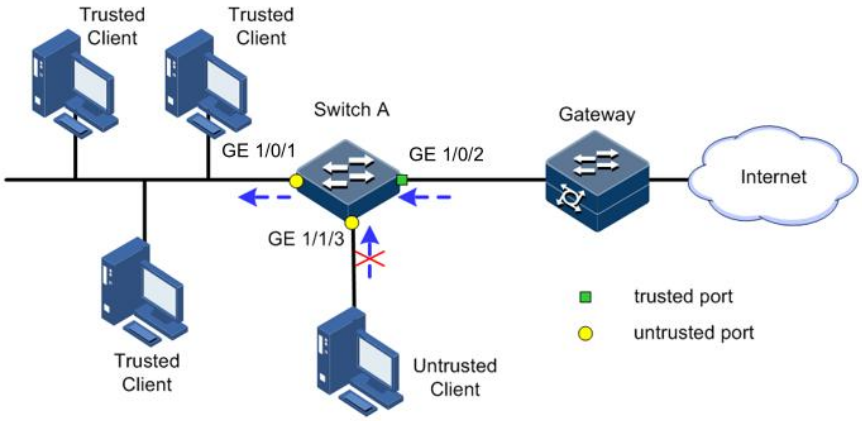
序号	检查项	说明
1	JX#**show nd-snooping config**	查看 ND Snooping 功能配置信息。
2	JX#**show nd-snooping user-bind**	查看 ND Snooping 用户绑定表。
3	JX#**show nd-snooping prefix**	查看 ND Snooping 前缀表。

8.8.6 配置 ND Snooping 示例

组网需求

如下图所示，某局域网络用户主机通过 Switch A 连接网关设备，由于网络中未部署 DHCPv6 服务器，这些主机需要根据网关分配给用户网络前缀信息，通过无状态地址自动配置方式获取 IPv6 地址。为防止非法用户发送 NA/NS/RS/RA 报文，导致合法主机无法获取 IPv6 地址，需要在 Switch 上开启 ND Snooping 功能，对非法的报文进行拦截。

图 8-10 配置 ND Snooping 组网示意图



配置步骤

步骤 1 在 Switch 上创建 VLAN 10 并激活。

配置 Switch。

```
JX#config
JX(config)#hostname SwitchA
SwitchA(config)#vlan 10
```

步骤 2 将 Switch A 的接口 GE 1/0/2 以 Access 模式加入 VLAN 10，设置接口 GE 1/0/1 为 Trunk 模式并允许 VLAN 10 通过。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type access
SwitchA(config-ge-1/0/2)#port default vlan 10
SwitchA(config-ge-1/0/2)#exit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 10
SwitchB(config-ge-1/0/1)#exit
```

步骤 3 全局和 VLAN 10 分别使能 ND Snooping 功能，配置 GE 1/0/1 为信任接口。

```
SwitchA(config)#nd-snooping start
SwitchA(config)#vlan 10
SwitchA(config-vlan-10)#nd-snooping enable
SwitchA(config-vlan-10)#exit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#nd-snooping enable
SwitchA(config-ge-1/0/1)#nd-snooping trust
SwitchA(config-ge-1/0/1)#exit
```

步骤 4 使能 ND 协议报文合法性检查功能。

```
SwitchA(config)#nd-snooping check na enable
SwitchA(config)#nd-snooping check ns enable
SwitchA(config)#nd-snooping check rs enable
```

检查结果

通过 **show nd-snooping config** 命令查看配置是否正确。

```
JX#show nd-snooping config
!
nd-snooping start
nd-snooping check na enable
nd-snooping check ns enable
nd-snooping check rs enable
!
vlan 10
 nd-snooping enable
!
interface ge 1/0/1
nd-snooping enable
nd-snooping trust
```

8.9 DHCP Snooping

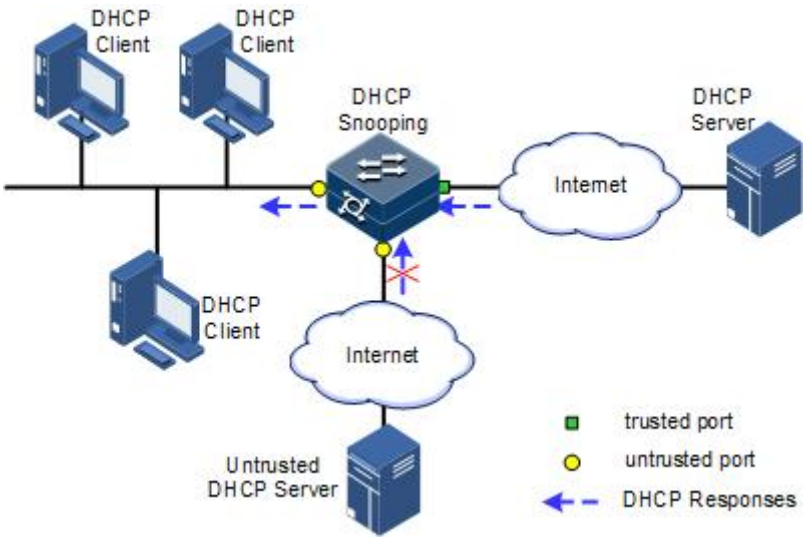
8.9.1 简介

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

- 保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址；

网络中如果存在私自架设的伪 DHCP 服务器，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。如图 8-11 所示，为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将接口设置为信任接口和不信任接口：信任接口正常转发接收到的 DHCP 报文；不信任接口接收到来自 DHCP 服务器的回应报文后将其丢弃。

图 8-11 DHCP Snooping 组网示意图



- 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

DHCP Snooping 通过监听请求和信任接口收到的回应报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、获取到的 IP 地址、与 DHCP 客户端连接的接口及该接口所属的 VLAN 等信息。利用这些信息可以实现：

- ARP Detection：根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。
- IP Source Guard：通过动态获取 DHCP Snooping 表项对接口转发的报文进行过滤，防止非法报文通过该接口。
- VLAN 映射：发送给用户的报文通过查找映射 VLAN 对应的 DHCP Snooping 表项中的 DHCP 客户端 IP 地址、MAC 地址和原始 VLAN 的信息，将报文的映射 VLAN 修改为原始 VLAN。

DHCP 报文中的 Option 字段记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。

如果设备配置了 DHCP Snooping 支持 Option 功能：

- 当设备接收到 DHCP 请求报文时，将根据报文中是否包含 Option 字段以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器；
- 当设备接收到 DHCP 回应报文时，如果报文中含有 Option 字段，则删除该字段，并转发给 DHCP 客户端；如果报文中不含有 Option 字段，则直接转发。

8.9.2 配置准备

场景

DHCP Snooping 作为 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

DHCP 报文中的 Option 字段记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。配置了 DHCP Snooping 支持 Option 功能的交换机设备可以根据报文中是否包含 Option 字段，对其进行相应的处理。

前提

无

8.9.3 DHCP Snooping 的缺省配置

设备上 DHCP Snooping 的缺省配置如下。

功能	缺省值
全局 DHCP Snooping 状态	禁止
接口 DHCP Snooping 状态	去使能
接口信任状态	不信任

功能	缺省值
DHCP Snooping 支持 Option 82	禁止

8.9.4 配置 DHCP Snooping

通常情况下，需要确保设备连接 DHCP 服务器侧的接口为信任状态，连接用户侧的接口为不信任状态。

对于启动了 DHCP Snooping 的设备，如果没有配置 DHCP Snooping 支持 Option 功能，则设备将不会对报文的 Option 字段进行任何处理。对于没有携带 Option 字段的报文，设备也不会进行插入处理。

缺省情况下设备所有接口的 DHCP Snooping 功能均已使能，但只有在使能全局 DHCP Snooping 功能后，接口的 DHCP Snooping 功能才会生效。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dhcp-snooping start**	使能全局 DHCP Snooping 功能。
3	JX(config)#**interface** *interface-type interface-number* JX(config)#**vlan** *vlan-id*	进入物理接口配置模式或者 VLAN 配置模式。
4	JX(config-ge-1/0/*)#**dhcp-snooping enable**	使能接口的 DHCP Snooping 功能，支持 QinQ 接口。
5	JX(config-ge-1/0/*)#**dhcp-snooping trust**	配置 DHCP Snooping 信任接口，仅在物理接口配置模式下生效。
6	JX(config-vlan-*)#**dhcp-snooping trust interface** *interface-type interface-number*	配置 DHCP Snooping 信任接口，仅在 vlan 配置模式下生效。
7	JX(config-ge-1/0/*)#**dhcp-snooping max-user-number** *number*	配置 DHCP Snooping 绑定表最大数量。
8	JX(config-ge-1/0/*)#**dhcp-snooping server-filter enable**	配置 DHCP Snooping 信任 server 配置功能
9	JX(config-ge-1/0/*)#**dhcp-snooping check user-bind enable**	配置 DHCP 报文进行绑定表匹配检测功能
10	JX(config-ge-1/0/*)#**dhcp-snooping check mac-address enable**	配置 DHCP 用户上送的请求报文头中的 MAC 地址是否合法功能
11	JX(config-ge-1/0/*)#**dhcp-snooping option82 enable**	配置 DHCP Snooping 支持 Option82 功能。
12	JX(config)#**exit**	返回全局配置模式。

8.9.5 配置 DHCP Snooping 支持 Option 82 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dhcp-snooping start**	使能全局 DHCP Snooping 功能。
3	JX(config)#**interface** *interface-type interface-number* JX(config)#**vlan** *vlan-id*	进入物理接口配置模式或者 VLAN 配置模式。
4	JX(config-ge-1/0/*)#**dhcp-snooping enable**	使能接口的 DHCP Snooping 功能。
5	JX(config-ge-1/0/*)#**dhcp-snooping option82 enable**	配置全局开启 DHCP Snooping 支持 Option 82 功能。
6	JX(config-ge-1/0/*)#**dhcp-snooping option82 {circuit-id | remote-id} format default**	指定配置 Option82 选项为默认格式
7	JX(config-ge-1/0/*)#**dhcp-snooping option82 {circuit-id | remote-id} format user-defined**	指定配置 Option82 选项的自定义内容。
8	JX(config-ge-1/0/*)#**exit**	返回全局配置模式。

8.9.6 配置 DHCPv6 Snooping

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dhcp-snooping start**	使能全局 DHCP Snooping 功能。
3	JX(config)#**interface** *interface-type interface-number* JX(config)#**vlan** *vlan-id*	进入物理接口配置模式或者 VLAN 配置模式。
4	JX(config-ge-1/0/*)#**dhcpv6-snooping enable**	使能接口的 DHCPv6 Snooping 功能。
5	JX(config-ge-1/0/*)#**dhcpv6-snooping trust**	配置 DHCPv6 Snooping 信任接口，仅在物理接口配置模式下生效。
6	JX(config-vlan-*)#**dhcpv6-snooping trust interface** *interface-type interface-number*	配置 DHCPv6 Snooping 信任接口，仅在 vlan 配置模式下生效。
7	JX(config-ge-1/0/*)#**dhcpv6-snooping max-user-number** { *number* | **default** }	配置 DHCPv6 Snooping 绑定表最大数量。

步骤	配置	说明
8	JX(config-ge-1/0/*)#**dhcpv6-snooping option18 enable**	使能 DHCPv6 Snooping 支持 Option18 功能。
9	JX(config-ge-1/0/*)#**dhcpv6-snooping option18 format user-defined** *txt*	指定配置 Option18 选项的自定义内容。
10	JX(config-ge-1/0/*)#**dhcpv6-snooping option18 format default**	指定配置 Option18 选项的自定义内容。
11	JX(config-ge-1/0/*)#**dhcpv6-snooping option37 enable**	使能 DHCPv6 Snooping 支持 Option37 功能。
11	JX(config-ge-1/0/*)#**dhcpv6-snooping option37 format user-defined**	指定配置 Option37 选项的自定义内容。
12	JX(config-ge-1/0/*)#**dhcpv6-snooping option37 format default**	指定配置 Option37 选项为默认格式。

8.9.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show dhcp-snooping config**	查看 DHCP Snooping 功能配置信息。
2	JX#**show dhcp-snooping user-bind**	查看 DHCP Snooping 绑定表信息。
3	JX#**show dhcp-snooping statistics**	查看 DHCP Snooping 的报文统计信息。
4	JX#**show dhcp-snooping interface**	查看 DHCP Snooping 的接口配置信息。
5	JX#**show dhcpv6-snooping config**	查看基于 ipv6 的 DHCP Snooping 功能配置信息。
6	JX#**show dhcpv6-snooping user-bind**	查看基于 ipv6 的 DHCP Snooping 绑定表信息。
7	JX#**show dhcpv6-snooping statistics**	查看基于 ipv6 的 DHCP Snooping 的报文统计信息。
8	JX#**show dhcpv6-snooping interface**	查看基于 ipv6 的 DHCP Snooping 的接口配置信息。

8.9.8 维护

用户可以通过以下命令，维护设备 DHCP Snooping 特性的运行情况和配置情况。

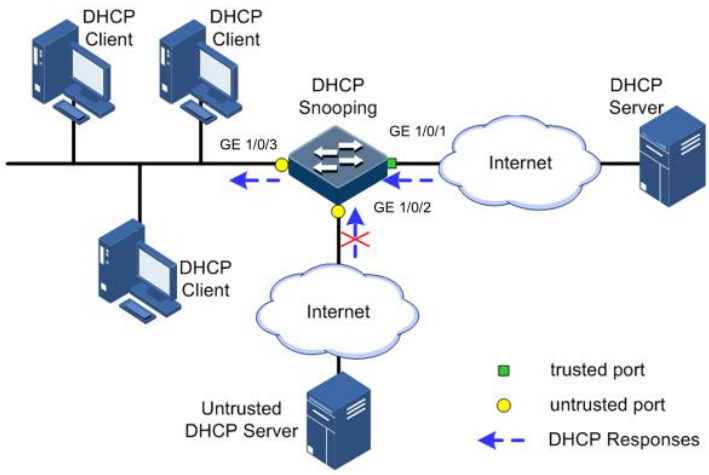
命令	描述
JX(config)#**reset dhcp-snooping user-bind** [*ip-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id*]	清除 IPv4 绑定表信息。
JX(config)#**reset dhcpv6-snooping user-bind** [*ipv6-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id*]	清除 IPv6 绑定表信息。

8.9.9 配置 DHCP Snooping 示例

组网需求

如图 8-12 所示，Switch 作为 DHCP Snooping 设备，需要保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，此外为了便于对客户端的管理，还需要设备支持 Option82 功能，在接口 GE 1/0/3 上配置电路 ID 子选项信息填充内容为 JX，远程 ID 子选项信息填充内容为 user01。

图 8-12 配置 DHCP Snooping 组网示意图



配置步骤

步骤 1 配置全局 DHCP Snooping 功能。

```
JX#config
JX(config)#dhcp-snooping start
```

步骤 2 配置信任接口。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dhcp-snooping enable
JX(config-ge-1/0/1)#dhcp-snooping trust
```

```
JX(config-ge-1/0/1)#exit
```

步骤 3 配置 DHCP Snooping 支持 Option82 功能并配置 Option82 字段。

```
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#dhcp-snooping enable
JX(config-ge-1/0/3)#dhcp-snooping option82 enable
JX(config-ge-1/0/3)#dhcp-snooping option82 remote-id format user-defined
'user01'
JX(config-ge-1/0/3)#dhcp-snooping option82 circuit-id format user-defined
'JX'
JX(config-ge-1/0/3)#exit
```

检查结果

通过 **show dhcp-snooping config** 命令查看 DHCP 服务器配置是否正确。

```
JX#show dhcp-snooping config
 Version : DHCPSNOOP_V7.00.03.00
!
dhcp-snooping start
!
interface ge 1/0/1
 dhcp-snooping enable
 dhcp-snooping trust
!
interface ge 1/0/3
 dhcp-snooping enable
 dhcp-snooping option82 enable
 dhcp-snooping option82 remote-id format user-defined 'user01'
 dhcp-snooping option82 circuit-id format user-defined 'JX'
……
```

8.10 IP Source Guard

8.10.1 简介

IP Source Guard 功能用于对接口收到的报文进行过滤控制，通常配置在接入用户侧的接口上，以防止非法用户报文通过，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了接口的安全性。

IP Source Guard 绑定表项

IP Source Guard 用于匹配报文的特征项包括源 IP 地址、源 MAC 地址和 VLAN 标签，并且可支持接口与以下特征项的组合（以下简称绑定表项）：

- 接口＋IP
- 接口＋IP＋MAC
- 接口＋IP＋VLAN
- 接口＋IP＋MAC＋VLAN

按照绑定表项的产生方式，IP Source Guard 分为以下两种：

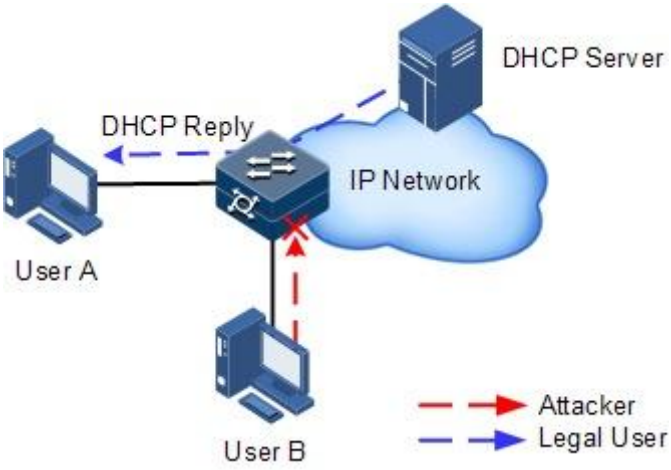
- 静态绑定：通过手工配置绑定信息，产生绑定表项来完成接口的控制功能，适用于主机数较少或者需要对某台主机进行单独绑定的情况。
- 动态绑定：通过 DHCP Snooping 自动获取绑定信息来完成接口的控制功能，适用于主机数较多并且采用 DHCP 进行动态主机配置的情况，可有效防止 IP 地址冲突和盗用等问题。

IP Source Guard 原理

IP Source Guard 的基本原理是在设备内部构建一个 IP 源绑定表，作为每个接口对接收数据包的检验依据。IP Source Guard 原理如下图所示，其转发原则如下：

- 所接收到的 IP 报文满足 IP 源绑定表中 Port/IP/MAC/VLAN 绑定表项的对应关系，则转发；
- 所接收到的 IP 报文为 DHCP 数据包，则转发；
- 所接收到的 IP 报文为其他情况，则丢弃。

图 8-13 IP Source Guard 功能示意图



当设备在转发 IP 报文时，将此 IP 报文中的源 IP、源 MAC、接口、VLAN 信息和绑定表的信息进行比较，如果信息匹配，说明是合法用户，则允许此报文正常转发；否则认为是攻击者，丢弃该用户发送的 IP 报文。

8.10.2 配置准备

场景

网络中常常存在针对 IP 源进行欺骗的攻击行为，如攻击者仿冒合法用户发送 IP 报文给服务器，或者伪造其他用户的源 IP 地址进行通信，从而导致合法用户不能正常获得网络服务。

通过 IP Source Guard 绑定功能，可以对接口转发的报文进行过滤控制，防止非法报文通过接口，从而限制了对网络资源的非法使用，如非法主机仿冒合法用户 IP 接入网络等，提高了接口的安全性。

前提

配置 IP Source Guard 之前，需要完成以下任务：

- 如果存在 DHCP 用户，则需要使能 DHCP Snooping 功能。

8.10.3 IP Source Guard 功能的缺省配置

设备上 IP Source Guard 功能的缺省配置如下。

功能	缺省值
接口 IP Source Guard 状态	禁止

8.10.4 配置 IP Source Guard 绑定功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**user-bind static ip** *ip-address/any* ***mac*** *mac-address/any* [**interface** *interface-type interface-number*] **vlan** *vlan-id/any*	配置静态绑定关系。
	JX(config)#**user-bind static ip6** *ipv6-address/any* ***mac*** *mac-address/any* [**interface** *interface-type interface-number*] **vlan** *vlan-id/any*	配置 IPv6 静态绑定关系。

8.10.5 配置 IP Source Guard 接口信任状态

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/*)#**ip source check user-bind enable**	使能接口 IP Source Guard 功能。

8.10.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show ip source check config	查看 IP Source Guard 功能配置信息。
2	JX#show ip source check interface	查看已使能 IP Source Guard 的接口信息

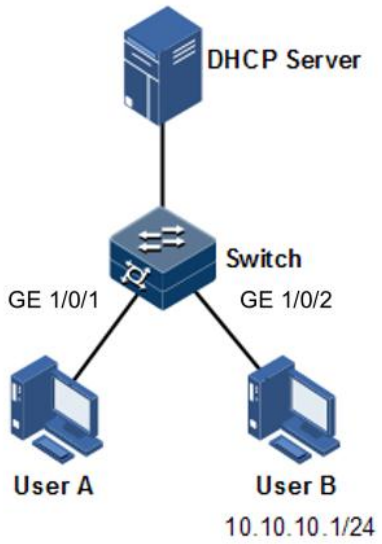
8.10.7 配置 IP Source Guard 示例

组网需求

如下图所示，为了防止 IP 地址盗用，需要在交换机上配置 IP Source Guard 功能，要求如下：

- 交换机允许接口 GE 1/0/1 上的所有 IP 报文通过；
- 接口 GE 1/0/2 允许指定 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0 的 IP 报文以及符合 DHCP Snooping 学习到的动态绑定关系的报文通过；
- 其它接口仅允许通过 DHCP Snooping 学习的动态绑定关系的报文通过。

图 8-14 IP Source Guard 应用组网示意图



配置步骤

步骤 1 配置 IP Source Guard 功能。

```
JX#config
```

```
JX(config)#int ge 1/0/2
JX(config-ge-1/0/2)#ip source check user-bind enable
JX(config-ge-1/0/2)#exit
JX(config)#int ge 1/0/1
JX(config-ge-1/0/1)#ip source check user-bind enable
JX(config-ge-1/0/1)#exit
```

步骤 2 配置静态绑定表项。

```
JX(config)# user-bind static ip 10.10.10.1 mac any interface ge 1/0/2
vlan any
```

步骤 3 接口 GE 1/0/2 和其他接口配置 DHCP snooping 功能。

检查结果

通过 **show ip source check config** 命令查看 IP Source Guard 配置结果。

```
JX#show ip source check config
!
user-bind static ip 10.10.10.1 mac any interface ge 1/0/2 vlan any
!
interface ge 1/0/2
ip source check user-bind enable
!
interface ge 1/0/1
ip source check user-bind enable
```

通过 **show ip source check interface** 命令查看已使能 IP Source Guard 的接口信息。

```
JX#show ip source check interface
Interface         Check-Item        Alarm    Limit      DropPkts
------------------------------------------------------------------------
ge-1/0/2          ip,mac,vlan       disable  100        0
ge-1/0/1          ip,mac,vlan       disable  100        0
------------------------------------------------------------------------
```

8.11 CPU 防攻击

8.11.1 配置准备

场景

当设备短时间内接收到大量的攻击报文，导致 CPU 满负荷运转，利用率达到 100%，会导致设备的正常功能无法运行。使用 CPU 防攻击功能可以有效限制进入 CPU 的报文的速率。

前提

无

8.11.2 配置 CPU 防攻击限速功能

注意

CPU 防攻击的配置对各协议模块的功能有重要的影响，建议不要轻易修改 CPU 保护的参数配置，只有专家才能修改相关配置。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)# **cpu-defend policy** *name*	配置 CPU 防攻击的策略，设备在启动的时候，会下发并绑定一个默认策略，默认策略不能修改，但是设备可以更改绑定的策略。
3	JX(config)#**cpu-defend policy test** JX(config-cpudefend-policy-test)#**car packet-type** { **arp** | **bfd** | **dhcpreply** | **dhcprequest** | **igmp** | **lacp** | **lldp** | **mld** | **stp-customer** | **telnet** | **...** } **pps** { *pps-value* | **default** }	配置该策略的指定协议包类型的限速值，整数形式，取值范围为 1～3000，默认值为 256。设备支持哪些协议包类型，取决于设备支持哪些协议。
4	JX(config)# **cpu-defend bind-policy** *name*	配置 CPU 防攻击的应用，字符形式，小于 31 个字符。绑定后的策略不能修改，只能先解绑定后再修改。

8.11.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show cpu-defend config**	查看 CPU 防攻击配置信息。
	JX#**show cpu-defend statistics**	查看 CPU 防攻击统计信息。

8.11.4 维护

命令	说明
JX(config)#**reset cpu-defend statistics**	清除全局的 CPU 防攻击统计信息。

8.12 MAC 认证

8.12.1 简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，无需安装客户端软件。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或密码。若该用户认证成功，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被设置为静默 MAC。在静默时间内，来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

- MAC 认证用户的账号格式：
  - MAC 地址账号：设备使用源 MAC 地址作为用户认证时的用户名和密码，或者使用 MAC 地址作为用户名，并配置密码。
  - 固定用户名账号：所有 MAC 地址认证用户均使用设备上指定的一个固定用户名和密码替代用户的 MAC 地址作为身份信息进行认证。
- 认证方式：

RADIUS 服务器认证方式进行 MAC 地址认证：当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作。

本地认证方式进行 MAC 地址认证：当选用本地认证方式进行 MAC 地址认证时，直接在设备上完成对用户的认证。需要在设备上配置本地用户名和密码。

- 重认证：

MAC 地址重认证是指设备周期性对端口上在线的 MAC 地址认证用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线。

8.12.2 缺省配置

设备上 MAC 认证的缺省配置如下：

功能	缺省值
全局 MAC 认证功能状态	禁止
接口 MAC 认证功能状态	禁止
全局认证方式	**pap**
802.1x 重认证功能状态	允许
802.1x 重认证定时器时间	1800s
MAC 认证静默定时器时间	60s

功能	缺省值
最大用户数	256

8.12.3 配置 MAC 认证

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**mac-authen { start | stop }**	使能或去使能全局 MAC 认证功能。
3	JX(config)#**mac-authen aaa authentication method** *method-name*	绑定全局 MAC 认证时的 AAA 方法，字符形式，小于 63 个字符。
5	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
6	JX(config-ge-1/0/*)#**mac-authen enable**	使能接口 MAC 认证功能。
7	JX(config-ge-1/0/*)#**mac-authen max-user** { *user-number* | **default** }	配置端口允许 MAC 认证的最大用户数，整数形式，取值范围为 1～128，默认值为 128。
8	JX(config-ge-1/0/*)#**nac guest-vlan** *vlan-id*	配置指定端口的 Guest VLAN，整数形式，取值范围为 1～4094。对 802.1x 协议和 mac 认证都生效。
9	JX(config-ge-1/0/*)#**mac-authen critical-vlan** *vlan-id*	配置指定端口的 MAC 认证 Critical VLAN，整数形式，取值范围为 1～4094。。
10	JX(config-ge-1/0/*)#**mac-authen restrict-vlan** *vlan-id*	配置指定端口的 MAC 认证 Restrict VLAN，整数形式，取值范围为 1～4094。。
11	JX(config-ge-1/0/*)#**mac-authen reauthenticate all user**	手动触发指定端口下 802.1x 用户进行重认证。
12	JX(config-ge-1/0/*)#**mac-authen delete all user**	强制将端口下 MAC 认证用户下线。
13	JX(config-ge-1/0/*)#**mac-authen quiet** { **disable** | **enable** }	使能或去使能端口 MAC 认证用户静默功能。
14	JX(config-ge-1/0/*)#**mac-authen quiet-times** { *times* | **default** }	配置端口 MAC 认证用户触发静默功能的认证失败次数，整数形式，取值范围为 3～10，默认 3 次。
15	JX(config-ge-1/0/*)#**mac-authen critical-vlan user aging** { **disable** | **enable** }	使能或去使能端口 MAC 认证超时用户老化功能。

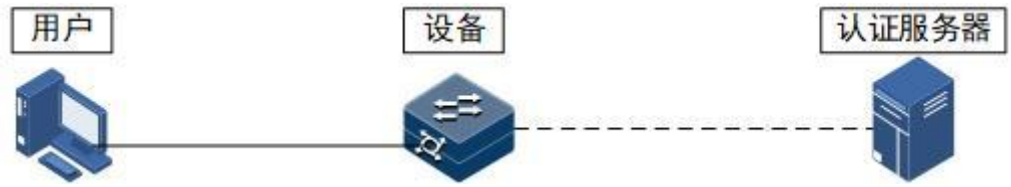
步骤	配置	说明
16	JX(config-ge-1/0/*)#**mac-authen critical-vlan user reauthenticate { disable | enable }**	使能或去使能端口 MAC 认证超时用户重认证功能。
17	JX(config-ge-1/0/*)#**mac-authen restrict-vlan user aging { disable | enable }**	使能或去使能端口 MAC 认证失败用户重认证功能。
18	JX(config-ge-1/0/*)#**mac-authen restrict-vlan user reauthenticate { disable | enable }**	使能或去使能端口 MAC 认证失败用户重认证功能。
19	JX(config)#**show mac-authen config**	查看 MAC 认证向配置。
20	JX(config)#**show mac-authen information**	查看 MAC 认证的全局信息。
21	JX(config)#**show mac-authen** *interface-type interface-number*	查看指定接口的 MAC 认证相关信息。
22	JX(config)#**show mac-authen user**	查看当前 MAC 认证的用户。

8.12.4 配置举例

组网需求

如下图所示，用户需要进行 MAC 认证，用户直接跟设备相连，设备可以访问认证服务器。

图 8-15 MAC 认证组网示意图



配置步骤

设备配置如下：

```
JX(config)#aaa
JX(config-aaa)#radius-server host server1 ip-address 192.168.5.66 key
12345
JX(config-aaa)#server-group grp1 radius-server server1
JX(config-aaa)#aaa authentication mac-authen method m1 first grp1
JX(config-aaa)#quit
JX(config)#mac-authen start
JX(config)#mac-authen aaa authentication method m1
JX(config)#mac-authen mode fixed-user username wwf password plain 12345
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#mac-authen enable
```

通过 **show mac-authen information** 命令查看 MAC 认证相关信息：

```
JX(config)#show mac-authen information
Max User Number                  : 128
  Default Max User Number          : 128
  Current User Number              : 0
  Auth Success User Number         : 0
  Auth Fail User Number            : 0
  Auth Timeout User Number         : 0
  UserName Passwor Format          : Fixed
  MacAdress UpperCase              : Disable
  MacAdress With Hypen             : Disable
  Mac Auth Method                  : Pap
  AAA Authentication Method        : m1
  AAA Accounting Method            : n/a
  Fixed User Name                  : wwf
  Fixed Password                   : 12345
```

检查结果

通过命令 **show mac-authen user** 查看当前 MAC 认证的用户：

```
JX(config)# show mac-authen user
 S:Success, F:Fail, T:Timeout, J:Join, A:Authenticate, O:Origin,
C:Current, L:Last
 Interface    Mac-Address      AuthNum(S/F/T)  Vlan(J/A/O)    Result(C/L)
 ge 1/0/1     0010:9400:0001    1/0/0          11/0/11        Success/None
```

8.13 DOS 防攻击

8.13.1 简介

畸形报文攻击防范

畸形报文攻击是通过向目标设备发送有缺陷的 IP 报文，使得目标设备在处理这样的 IP 报文时出错和崩溃，给目标设备带来损失。畸形报文攻击防范是指设备实时检测出畸形报文并予以丢弃，实现对本设备的保护。

分片报文攻击防范

分片报文攻击是通过向目标设备发送分片出错的报文，使得目标设备在处理分片错误的报文时崩溃、重启或消耗大量的 CPU 资源，给目标设备带来损失。分片报文攻击防范是指设备实时检测出分片报文并予以丢弃或者限速处理，实现对本设备的保护。

泛洪攻击防范

泛洪攻击是指攻击者在短时间内向目标设备发送大量的虚假报文，导致目标设备忙于应付无用报文，而无法为用户提供正常服务。

泛洪攻击防范是指设备实时检测出泛洪报文并予以丢弃或者限速处理，实现对本设备的保护。

泛洪攻击主要分为 TCP SYN 泛洪攻击、UDP 泛洪攻击和 ICMP 泛洪攻击。

- TCP SYN 泛洪攻击

TCP SYN 攻击利用了 TCP 三次握手的漏洞。在 TCP 的 3 次握手期间，当接收端收到来自发送端的初始 SYN 报文时，向发送端返回一个 SYN+ACK 报文。接收端在等待发送端的最终 ACK 报文时，该连接一直处于半连接状态。如果接收端最终没有收到 ACK 报文包，则重新发送一个 SYN+ACK 到发送端。如果经过多次重试，发送端始终没有返回 ACK 报文，则接收端关闭会话并从内存中刷新会话，从传输第一个 SYN+ACK 到会话关闭大约需要 30 秒。

在这段时间内，攻击者可能将数十万个 SYN 报文发送到开放的端口，并且不回应接收端的 SYN+ACK 报文。接收端内存很快就会超过负荷，且无法再接受任何新的连接，并将现有的连接断开。

设备对 TCP SYN 攻击处理的方法是在使能了 TCP SYN 泛洪攻击防范后对 TCP SYN 报文进行速率限制，保证受到攻击时设备资源不被耗尽。

- UDP 泛洪攻击

UDP 泛洪攻击是指攻击者在短时间内向目标设备发送大量的 UDP 报文，导致目标设备负担过重而不能处理正常的业务。UDP 泛洪攻击分为以下两类：

•Fraggle 攻击

Fraggle 攻击的原理是攻击者发送源地址为目标主机地址，目的地址为广播地址，目的端口号为 7 的 UDP 报文。如果该广播网络中有很多主机都起用了 UDP 响应请求服务，目的主机将收到很多回复报文，造成系统繁忙，达到攻击效果。

使能泛洪攻击防范功能后，设备默认 UDP 端口号为 7 的报文是攻击报文，直接将其丢弃。

- UDP 诊断端口攻击

攻击者对 UDP 诊断端口（7-echo，13-daytime，19-Chargen 等 UDP 端口）发送报文，如果同时发送的数据包数量很大，造成泛洪，可能影响网络设备的正常工作。

使能泛洪攻击防范功能后，设备将 UDP 端口为 7、13 和 19 的报文认为是攻击报文，直接丢弃。

- ICMP 泛洪攻击

通常情况下，网络管理员会用 Ping 程序对网络进行监控和故障排除，大概过程如下：

  - 1.源设备向接收设备发出 ICMP 响应请求报文；
  - 2.接收设备接收到 ICMP 响应请求报文后，会向源设备回应一个 ICMP 应答报文。

如果攻击者向目标设备发送大量的 ICMP 响应请求报文，则目标设备会忙于处理这些请求，而无法继续处理其他的数据报文，造成对正常业务的冲击。

设备针对 ICMP 泛洪攻击进行 CAR（Committed Access Rate）限速，保证 CPU 不被攻击，保证网络的正常运行。

8.13.2 配置准备

场景

设备经常会受到不同类型的网络攻击，这样会导致设备资源使用率过高，影响网络服务。为保障给用户提供安全的网络服务，在设备上部署 Dosantiattack 功能，主要防范的攻击类型包括：

- 畸形报文攻击防范，防止畸形报文攻击。
- 分片报文攻击防范，限制分片报文的速率，防止分片报文对 CPU 造成攻击，占用过多 CPU 和设备资源。
- 泛洪攻击防范，包括以下三种：
  - TCP SYN 泛洪攻击防范，限制 TCP SYN 报文的速率，防止 CPU 处理 TCP SYN 报文占用过多资源；
  - UDP 泛洪攻击防范，对特定端口发送的 UDP 报文直接丢弃；
  - ICMP 泛洪攻击防范，限制 ICMP 泛洪攻击报文的上送速率，防止 CPU 处理 ICMP 泛洪攻击报文占用过多资源。

前提

无

8.13.3 DOS 防攻击功能的缺省配置

设备上 DOS 防攻击功能的缺省配置如下。

功能	缺省值
Dosantiattack 全局功能状态	禁用
畸形报文攻击防范功能	禁用
分片报文攻击防范功能	禁用
分片报文发送速率	155000000bit/s
TCP Syn 攻击防范功能	禁用
TCP Syn 泛洪报文发送速率	155000000bit/s
UDP 泛洪攻击防范功能	禁用
ICMP 泛洪攻击防范功能	禁用
ICMP 泛洪报文发送速率	155000000bit/s

8.13.4 配置畸形报文攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit abnormal enable**	使能畸形报文攻击防范功能。

8.13.5 配置分片报文攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit fragment enable**	使能畸形报文攻击防范功能。
3	JX(config)#**dos-antiattack pkt-limit fragment cir** { **kbps**|**mbps**|**gbps** } *cir-number* JX(config)#**dos-antiattack pkt-limit fragment pps** *pps-number*	限制分片报文接收的速率。

8.13.6 配置 TCP SYN 泛洪攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit tcp-syn enable**	使能 TCP SYN 泛洪攻击防范功能。
3	JX(config)#**dos-antiattack pkt-limit tcp-syn cir** { **kbps**|**mbps**|**gbps** } *cir-number* JX(config)#**dos-antiattack pkt-limit tcp-syn pps** *pps-number*	限制 TCP SYN 报文接收的速率。

8.13.7 配置 UDP 泛洪攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit udp-flood enable**	使能 UDP 泛洪攻击防范功能。

8.13.8 配置 ICMP 泛洪攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit icmp-flood enable**	使能 ICMP 泛洪攻击防范功能。
3	JX(config)#**dos-antiattack pkt-limit icmp-flood cir** { **kbps**|**mbps**|**gbps** } *cir-number* JX(config)#**dos-antiattack pkt-limit icmp-flood pps** *pps-number*	限制 ICMP 泛洪攻击报文接收的速率。

8.13.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

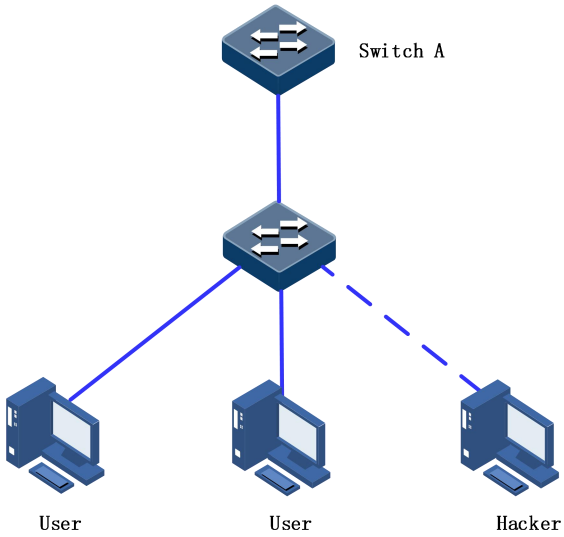
序号	检查项	说明
1	JX#**show dos-antiattack config**	查看 Dos 防攻击配置信息。
2	JX#**show dos-antiattack statistics**	查看 Dos 防攻击统计数据。

8.13.10 配置 DOS 防攻击示例

组网需求

如果局域网内存在 Hacker 向 SwitchA 发起畸形报文攻击、分片报文攻击和泛洪攻击，将会造成 SwitchA 瘫痪。为了预防这种情况，管理员希望通过在 SwitchA 上部署各种攻击防范措施来为用户提供安全的网络环境，保障正常的网络服务。

图 8-16 DOS 防攻击应用组网示意图



配置步骤

步骤 1 配置 DOS 防攻击功能。

```
JX#config
JX(config)#dos-antiattack pkt-limit enable
```

步骤 2 配置畸形报文攻击防范。

```
JX(config)#dos-antiattack pkt-limit abnormal enable
```

步骤 3 配置分片报文攻击防范，并限制分片报文接收的速率为 15kbit/s。

```
JX(config)#dos-antiattack pkt-limit fragment enable
JX(config)#dos-antiattack pkt-limit fragment cir kbps 15
```

步骤 4 配置 TCP SYN 攻击防范，并限制 TCP SYN 报文接收的速率为 15kbit/s。

```
JX(config)#dos-antiattack pkt-limit tcp-syn enable
JX(config)#dos-antiattack pkt-limit tcp-syn cir kbps 15
```

步骤 5 配置 UDP 泛洪攻击防范。

```
JX(config)#dos-antiattack pkt-limit udp-flood enable
```

步骤 6 配置 ICMP 泛洪攻击防范，并限制 ICMP 泛洪报文接收的速率为 15kbit/s。

```
JX(config)#dos-antiattack pkt-limit icmp-flood enable
JX(config)#dos-antiattack pkt-limit icmp-flood cir kbps 15
```

检查结果

通过 **show dos-antiattack config** 命令查看 DOS 防攻击配置结果。

```
JX#show dos-antiattack config
!
!
dos-antiattack pkt-limit enable
```

```
!
dos-antiattack pkt-limit abnormal enable
dos-antiattack pkt-limit fragment enable
dos-antiattack pkt-limit fragment cir kbps 15
dos-antiattack pkt-limit tcp-syn enable
dos-antiattack pkt-limit tcp-syn cir kbps 15
dos-antiattack pkt-limit udp-flood enable
dos-antiattack pkt-limit icmp-flood enable
dos-antiattack pkt-limit icmp-flood cir kbps 15
```

9 可靠性

本章介绍了网络可靠性的基本原理和配置过程，并提供相关的配置案例。

- 链路聚合
- G.8031
- G.8032
- STP/RSTP
- MSTP
- 环路检测
- 端口备份
- 端口隔离
- L2CP
- BFD
- 链路震荡保护
- 接口环回

9.1 链路聚合

9.1.1 简介

链路聚合通过将多个物理以太网接口聚合在一起形成一个逻辑上的聚合组，并把同一聚合组内的多条物理链路视为一条逻辑链路。链路聚合可以实现流量在聚合组各成员接口之间负载分担，在有效提高设备之间链路可靠性的同时，还在不进行硬件升级的条件下增大了带宽。

按照聚合方式的不同，设备支持以下四种链路聚合方式：

- 手工聚合方式

聚合组中所有接口都参与数据转发，平均分担负载流量，适用于两个直连设备，且一端设备无法使用 LACP 协议的情况。

- 手工主备方式链路聚合方式

聚合组中共有 2 个接口，2 个接口之间形成备份，一个处于 Active 状态，另外一个处于 Shutdown 状态。适用于一端设备无法使用 LACP 协议的情况。

- 静态 LACP 聚合方式

聚合组通过 LACP 协议来选择主动端和活动接口。活动接口用于转发数据，而非活动接口用于备份链路。适用于两端设备均支持 LACP 协议的情况。

- 静态 LACP 主备方式链路聚合方式

聚合组中共有 2 个接口，2 个接口之间形成备份，一个处于 Active 状态，另外一个处于 Shutdown 状态。适用于两端设备均支持 LACP 协议的情况。

9.1.2 配置准备

场景

当需要为 2 台设备之间的链路提供更高的通讯带宽和更高的可靠性时，可以配置选择手工模式或者静态 LACP 链路聚合功能。

前提

- 在配置链路聚合之前，需配置接口的物理参数，使接口的物理层状态为 Up。
- 在同一个链路聚合组中，参与负载分担的成员接口必须有一致的配置，否则数据转发存在问题。这些配置主要包括 QoS、QinQ、VLAN、接口属性、MAC 地址学习几个方面：
  - QoS 配置一致：流量监管、流量整形、拥塞避免、接口限速、SP 队列、WRR 队列调度、WFQ 队列、接口优先级、接口信任模式。
  - QinQ 配置一致：接口的 QinQ 功能使能/禁用状态、添加的外层 VLAN Tag、不同内层 VLAN ID 添加外层 VLAN Tag 的策略。
  - VLAN 配置一致：接口上允许通过的 VLAN、接口缺省 VLAN ID、接口的链路类型（即 Trunk、Hybrid、Access 类型）、子网 VLAN 配置、协议 VLAN 配置、VLAN 报文是否带 Tag 配置。
  - 接口属性配置一致：接口是否加入隔离组、接口速率、双工模式、链路 up/down 状态。
  - MAC 地址学习配置一致：是否使能 MAC 地址学习功能、接口是否具有最大学习 MAC 地址个数的限制。

9.1.3 缺省配置

设备上链路聚合的缺省配置如下。

功能	缺省值
负载均衡模式	**src-dst-mac** 模式
LACP 系统优先级	32768
LACP 接口优先级	32768

功能	缺省值
LACP 接口模式	**active**
LACP 超时模式	**slow**
最小活动接口数	1
最大活动接口数	8

9.1.4 配置手工链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**int eth-trunk** *trunk-number*	进入聚合组配置模式。
3	JX(config-eth-trunk-*)#**mode manual**	配置链路聚合组的工作模式为手工链路聚合。
4	JX(config-eth-trunk-*)#**active-linknumber** { **max**|**min** } { *number*|*default* }	配置 LACP 链路聚合组最大或最小的活跃链路数量。 缺省情况下，最大活跃链路数为 8，最小活跃链路数为 1。
5	JX(config-eth-trunk-*)#**add interface** *interface-type interface-number*	将接口加入聚合
6	JX(config-eth-trunk-*)#remove **interface** *interface-type interface-number*	将接口移除出聚合
7	JX(config-ge-1/0/*)#**join eth-trunk** *trunk-id*	将接口加入聚合
8	JX(config-ge-1/0/*)#**no join eth-trunk** *trunk-id*	将接口移除出聚合
9	JX(config-eth-trunk-*)#**exit**	返回全局配置模式。

9.1.5 配置手工主备链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**int eth-trunk** *trunk-number*	进入聚合组配置模式。

步骤	配置	说明
3	JX(config-eth-trunk-*)#**mode manual active-standby**	配置链路聚合组的工作模式为手工主备链路聚合。
4	JX(config-eth-trunk-*)#**add primary interface** *interface-type interface-number*	将主接口加入聚合
5	JX(config-eth-trunk-*)#**add secondary interface** *interface-type interface-number*	将备接口加入聚合
6	JX(config-eth-trunk-*)#**remove interface** *interface-type interface-number*	将接口移除出聚合
7	JX(config-eth-trunk-*)#**revert** {enable|disable}	修改主备聚合的回切使能
8	JX(config-eth-trunk-*)#**wait-to-restore** *time-interval*	修改主备聚合的回切等待时间，单位秒

9.1.6 配置静态 LACP 链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**lacp system-priority** *system-priority*	配置 LACP 协议优先级，优先级高的一端为主动端，LACP 按主动端的配置情况选择活动接口和备份接口。数值越小优先级越高，系统 LACP 优先级相同时，选择系统 MAC 地址小的作为主动端。 缺省情况下，系统的 LACP 优先级为 32768。
3	JX(config)#**int eth-trunk** *trunk-number*	进入聚合组配置模式。
4	JX(config-eth-trunk-*)#**mode lacp-static**	配置链路聚合组的工作模式为静态 LACP 链路聚合。
5	JX(config-eth-trunk-*)#**lacp timeout** { **fast** | **slow** }	配置 LACP 超时模式。 缺省情况下，LACP 超时模式为慢速模式。
6	JX(config-eth-trunk-*)#**active-linknumber** { **max**|**min** } { *number*|*default* }	配置 LACP 链路聚合组最大或最小的活跃链路数量。 缺省情况下，最大活跃链路数为 8，最小活跃链路数为 1。
7	JX(config-eth-trunk-*)#**lacp preempt enable**	使能链路聚合组的优先级抢占功能。

步骤	配置	说明
8	JX(config-eth-trunk-*)#**lacp preempt delay** *time*	配置端口延时抢占。
9	JX(config-eth-trunk-*)#**add interface** *interface-type interface-number*	将接口加入聚合
10	JX(config-eth-trunk-*)#remove **interface** *interface-type interface-number*	将接口移除出聚合
11	JX(config-ge-1/0/*)#**join eth-trunk** *trunk-id*	将接口加入聚合
12	JX(config-ge-1/0/*)#**no join eth-trunk** *trunk-id*	将接口移除出聚合
13	JX(config-ge-1/0/*)#**lacp priority** *priority*	配置接口的 LACP 协议优先级，接口协议优先级影响 LACP 协议的缺省接口的选举，数值越小优先级越高。 缺省情况下，系统的 LACP 优先级为 32768。
14	JX(config-ge-1/0/*)#**exit**	返回全局配置模式。

说明

- 在静态 LACP 链路聚合组中，成员接口可以处于 Active 或 Standby 两种状态。Active 接口和 Standby 接口都能收发 LACP 协议报文，但 Standby 接口不能转发用户报文。
- 系统按照是否发现邻居、接口速率最大、接口 LACP 协议优先级最高、接口号最小的顺序选择缺省接口，缺省接口处于 Active 状态，与缺省接口具有相同速率、相同对端设备和对端设备操作 key 的接口也处于 Active 状态，其他接口则处于 Standby 状态。

9.1.7 配置聚合组负载分担算法

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**int eth-trunk** *trunk-number*	进入聚合组配置模式。

步骤	配置	说明
3	JX(config-eth-trunk-*)#**load-balance-profile default** JX(config-load-balance-profile-default)#**l2 field { src-mac|dst-mac|l2-protocol|vlan|src-port|dst-port|eth-type|outer-vlan|srcdst-mac|all|default }** JX(config-load-balance-profile-default)#**l3 field { src-ip|dst-ip|srcdst-ip|vlan|l4-srcport|l4-dstport|protocol|src-port|dst-port|src-mac|dst-mac|all|default}**	基于全局配置链路聚合组的负载均衡模式。 缺省情况下，l2 模式下系统基于 **src-mac、dst-mac** 字段进行负载均衡，l3 模式下系统基于所有字段进行负载均衡。

说明

- 链路聚合组的负载均衡模式仅针对已知单播报文生效。

9.1.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

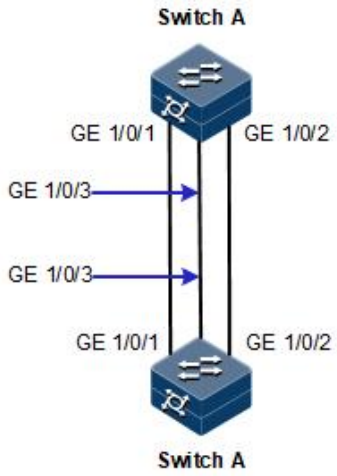
序号	检查项	说明
1	JX#**show lacp eth-trunk** *trunk-number*	查看本端系统 LACP 协议接口状态、标志、接口优先级、管理 key、操作 key 和接口状态机状态。邻居 LACP 协议信息，包括标志、接口优先级、设备 ID、Age、操作键值、接口号、接口状态机状态。
2	JX#**show lacp statistics interface eth-trunk** *trunk-number*	查看接口 LACP 协议统计信息，包括 LACP 报文的总收发数、Marker 报文的收发数、Marker Response 报文的收发数和错误报文数。
3	JX#**show lacp information**	查看本端系统的 LACP 系统优先级，MAC 地址，各定时器时间
4	JX#**show** interface **eth-trunk** *trunk-number*	查看当前系统是否使能聚合链路、链路聚合负载均衡模式、当前所有聚合组设置的组成员接口列表和当前生效的成员接口列表等信息。 **说明** 当前生效的成员接口是指组成员接口中接口状态为 Up 的接口列表。

9.1.9 配置静态 LACP 方式的链路聚合示例

组网需求

如下图所示，为提高 Switch A 与 Switch B 之间链路的可靠性，在 Switch A 与 Switch B 之间配置静态 LACP 方式的链路聚合，将 GE 1/0/1、GE 1/0/2 和 GE 1/0/3 加入链路聚合组。

图 9-1 静态 LACP 方式链路聚合应用组网示意图



配置步骤

步骤 1 在 Switch A 上配置静态 LACP 链路聚合组，并将 Switch A 配置成主动端。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#int eth-trunk 1
SwitchA(config-eth-trunk-1)#mode lacp-static
SwitchA(config-eth-trunk-1)#add interface ge 1/0/1
SwitchA(config-eth-trunk-1)#add interface ge 1/0/2
SwitchA(config-eth-trunk-1)#add interface ge 1/0/3
SwitchA(config-eth-trunk-1)#exit
```

步骤 2 在 Switch B 上配置静态 LACP 链路聚合组。

```
JX#hostname SwitchB
SwitchB#configure
SwitchB(config)#int eth-trunk 1
SwitchB(config-eth-trunk-1)#mode lacp-static
SwitchB(config-eth-trunk-1)#add interface ge 1/0/1
SwitchB(config-eth-trunk-1)#add interface ge 1/0/2
SwitchB(config-eth-trunk-1)#add interface ge 1/0/3
SwitchB(config-eth-trunk-1)#exit
```

检查结果

在 Switch A 上通过 **show lacp eth-trunk 1** 查看静态 LACP 方式链路聚合全局配置是否正确。

```
SwitchA#show lacp eth-trunk 1
-------------------------------------------------------------------------------
------------
  LACP Status                 : master
  System Priority             : 1000
  System Mac Address          : f0:f1:f2:f3:01:01
  Member ports number         : 3
  Max Active ports number      : 8
  LACP timeout                : slow
  Preempt state               : disable
  Preempt delay               : 30(s)

 ge-1/0/1 :
    Port Status  : Up and bind
    Local information:
      Mode     Flags   PortPri   AdminKey  OperKey   PortId  State   Status
      active   slow    32768     1         1         449     0x3d    selected
    Partner information:
      SysPri    Flags   PortPri   AdminKey  OperKey   PortId  State   DeviceID
      32768     slow    32768     0         1         449     0x3d
0xf0f1f2f30201

 ge-1/0/2 :
    Port Status  : Up and bind
    Local information:
      Mode     Flags   PortPri   AdminKey  OperKey   PortId  State   Status
      active   slow    32768     1         1         450     0x3d    selected
    Partner information:
      SysPri    Flags   PortPri   AdminKey  OperKey   PortId  State   DeviceID
      32768     slow    32768     0         1         450     0x3d
0xf0f1f2f30201

 ge-1/0/3 :
    Port Status  : Up and bind
    Local information:
      Mode     Flags   PortPri   AdminKey  OperKey   PortId  State   Status
      active   slow    32768     1         1         451     0x3d    selected
    Partner information:
      SysPri    Flags   PortPri   AdminKey  OperKey   PortId  State   DeviceID
      32768     slow    32768     0         1         451     0x3d
0xf0f1f2f30201
-------------------------------------------------------------------------------
------------
```

9.2 G.8031

9.2.1 简介

G.8031 是 ITU-T 基于 VLAN 的以太网技术定义的线性保护倒换标准。在保护切换机制中，对工作资源都分配相应的保护资源，如路径和带宽等。相对于 IEEE 定义的生成树保护技术，G.8031 定义的保护技术简单快速，以一种可预测的方式实现网络资源切换，更易于运营商有效地规划网络及明了网络的活动状态，实现电信级的运营。

G.8031 定义了 1+1 和 1:1 两种保护结构，在 1+1 结构中每一个保护资源都对应着一个工作资源，在保护域内，1+1 结构采用双发单收的保护机制；1:1 结构采用保护资源与工作资源彼此切换的机制。

- 故障检测机制

G.8031 采用 Y.1731 或 IEEE 802.1ag 中定义的连续性检测(CC)进行链路双向转发检测，能够定位故障点并检测故障是单向还是双向的，并且用于保护转换时，CC 帧默认的传输周期是 3.33 ms（即每秒 300 帧的传输速率）。

两个相邻节点间周期性的从物理端口发送连续性检测(CC)帧以检测故障，当一个节点在特定的时间内检测到 CC 帧丢失，即检测到了一个故障。

节点从检测到故障的端口发送 RDI(Remote Defect Indication)帧，如果是单向故障，链路下行的节点将检测到该 RDI 帧。

- 1+1 保护结构

在 1+1 结构中，保护连接是每条工作连接专用的，工作连接与保护连接在保护域的源端进行桥接。业务在工作和保护连接上同时发向保护域的宿端，在宿端，选择器基于缺陷指示来选择接收来自工作或保护连接上的业务。

1+1 以太网线性保护的倒换类型包括单向倒换和双向倒换。单向倒换时只有受影响的连接方向倒换至保护路径，两端的选择器是独立的，不需要 APS 信令支持。双向倒换的机制与单向类似，通常需要 APS 信令在两端协调。单向保护可以防止在两个独立方向上的单通故障。

1+1 以太网线性保护的操作类型可以是不可恢复或可恢复的。在可恢复模式下，故障链路恢复时，启动 WTR 定时器，WTR 超时后，选择器切换到工作链路；在不可恢复模式下，即使故障链路恢复，选择器仍然连接到保护链路。

- 1:1 保护结构

在 1:1 结构中，保护连接是每条工作连接专用的，被保护的工作业务由工作或保护连接进行传送。工作和保护连接的选择方法基于缺陷指示机制。

1:1 以太网线性保护的倒换类型也包括单向倒换和双向倒换，操作类型可以是可恢复的，也可以是不可恢复的，双向倒换时受影响的和未受影响的连接方向均倒换至保护路径，而单向倒换仅受影响的的连接方向均倒换至保护路径。倒换时源端和宿端连接器需要切换到同一个连接，因此需要自动保护倒换协议 APS 用于协调连接的两端。

在 1:1 保护倒换模式下，基于本地或近端信息和来自另一端或远端的 APS 协议信息，保护倒换由保护域源端选择器桥接和宿端选择器共同来完成。

使用连接性检查包检测工作和保护连接故障，当工作连接故障时，检测到故障的一端选择器切换到保护连接上，同时发送 APS 通知对端，源端收到 APS 同步倒换。

9.2.2 配置准备

场景

无

前提

在配置 G.8031 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up；
- 创建 VLAN；
- 将接口加入 VLAN。

9.2.3 G.8031 的缺省配置

设备上 G.8031 的缺省配置如下。

功能	缺省值
G.8031 模式	返回模式
WTR 定时器	5min
HOLDOFF 定时器	0

9.2.4 创建 G.8031 保护组

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**g8031 instance** *instance-id*	创建 G8031 实例并进入配置节点
3	JX(config-g8031-instance-*)#**control-vlan** *vlan-id*	指定控制 vlan，如果配置了 **revertive dsiable**，则保护组变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护组处于返回模式。
4	JX(config-g8031-instance-*)#**data-vlan** *vlan-id*	指定数据 vlan

步骤	配置	说明
5	JX(config-g8031-instance-*)# **working-port interface** *interface-type interface-number*	配置端口并指定为工作端口
6	JX(config-g8031-instance-*)# **protection-port interface** *interface-type interface-number*	配置端口并指定为保护端口
7	JX(config-g8031-instance-*)#**wtr-timer** *wtr-time*	配置 WTR 定时器。在返回模式下当工作链路故障恢复时，等待 WTR 定时器超时之后，才会恢复到工作链路上工作。
8	JX(config-g8031-instance-*)#**holdoff-timer** *holdoff-time*	配置环 HOLDOFF 定时器后，当工作链路故障时，系统会延时上报故障，即延时一段时间后再倒换到保护链路，可以防止工作链路震荡引起的频繁倒换。 **说明** HOLDOFF 定时器配置值较大时会影响 50ms 倒换性能，所以推荐使用缺省值 0。

9.2.5 配置 G.8031 倒换控制

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config-g8031-instance-*)#**protection-switch force-switch**	配置流量强制倒换。 强制倒换可配置在多个环节点的多个接口上。
3	JX(config-g8031-instance-*)#**protection-switch manual-switch**	配置流量手工倒换，优先级低于强制倒换和工作链路故障时产生的自动倒换。 手工倒换只能配置在同一个环节点的一个接口上。
4	JX(config-g8031-instance-*)#**protection-switch clear**	配置流量倒换清除。

9.2.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show g8031 interface**	查看 G.8031 接口状态信息。
2	JX#**show g8031 instance**	查看 G.8031 状态信息。

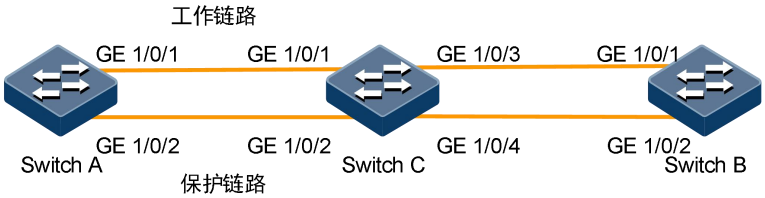
9.2.7 配置 G.8031 保护示例

组网需求

如图 9-2 所示，为提高以太网络的可靠性，Switch A、Switch B、Switch C 三台设备组成 G.8031 保护链路。

协议控制 VLAN 为 2，阻塞的 VLAN 范围为 2～10。

图 9-2 G.8031 组网示意图



配置步骤

步骤 1 配置接口加入 VLAN 2～VLAN 10。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#interface ge 1/0/1 to ge 1/0/2
SwitchA(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan 2-10
SwitchA(config-ge-1/0/1->ge-1/0/2)#exit
```

Switch B 配置同 Switch A

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#configure
SwitchC(config)#interface ge 1/0/1 to ge 1/0/4
SwitchC(config-ge-1/0/1->ge-1/0/4)#port link-type trunk
SwitchC(config-ge-1/0/1->ge-1/0/4)#port trunk allow-pass vlan 2-10
SwitchC(config-ge-1/0/1->ge-1/0/4)#exit
```

步骤 2 创建保护组。

配置 Switch A。

```
SwitchA(config)#g8031 instance 1
SwitchA(config-g8031-instance-1)#control-vlan 2
SwitchA(config-g8031-instance-1)#data-vlan 2-10
SwitchA(config-g8031-instance-1)#working-port interface ge 1/0/1
SwitchA(config-g8031-instance-1)#protection-port interface ge 1/0/2
```

配置 Switch B。

```
SwitchC(config)#g8031 instance 1
SwitchC(config-g8031-instance-1)#control-vlan 2
SwitchC(config-g8031-instance-1)#data-vlan 2-10
SwitchC(config-g8031-instance-1)#working-port interface ge 1/0/1
SwitchC(config-g8031-instance-1)#protection-port interface ge 1/0/2
```

检查结果

在设备上通过 **show g8031 interface** 查看 G.8031 保护是否生效。

以 Switch A 为例，状态信息如下：

```
SwitchA#show g8031 interface
Instance Interface      Role        Active  Operate   Forward    RxCount
TxCount
-------------------------------------------------------------------------
--------------------------
1       ge-1/0/1       working      active  working   forwarding  0        0
1       ge-1/0/2       protection    standby working   blocking    0        6
-------------------------------------------------------------------------
--------------------------
```

手动断开链路模拟故障，在 Switch A 上再次使用命令查看 G.8031 保护状态

```
SwitchA#show g8031 interface
Instance Interface      Role        Active  Operate   Forward    RxCount
TxCount
-------------------------------------------------------------------------
--------------------------
1       ge-1/0/1       working      standby failed    blocking  0        0
1       ge-1/0/2       protection    active  working   forwarding   0      6
-------------------------------------------------------------------------
--------------------------
```

9.3 G.8032

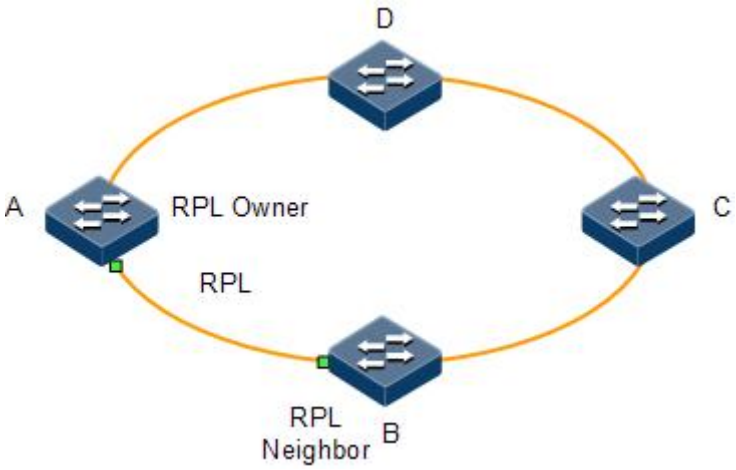
9.3.1 简介

G.8032 以太网环网保护倒换（Ethernet Ring Protection Switching，ERPS）是基于 ITU-T G.8032 标准的 APS 协议，是一种专门应用于以太网环的链路层协议。正常情况下，它在以太网环中能够防止数据环路引起的广播风暴。当以太网环上链路或设备故障时，能迅速切换到备份链路，保证业务快速恢复。

G.8032 利用环网内专用的控制 VLAN 传递环网控制信息，同时结合环网本身的拓扑特点，在网络发生故障时快速发现，并启用备份链路从而做到快速恢复。

相关概念

图 9-3 G.8032 环网示意图



如图 9-3 所示，G.8032 环网的一些基本概念如下。

- RPL：RPL（Ring Protection Link，环网保护链路）是 RPL 节点间的链路，正常状态下阻塞该链路的相应接口以避免形成环路。一个环网只有一条 RPL。
- RPL Owner：与 RPL 相连的一个环网节点称为 RPL Owner，由用户指定，用于控制 RPL 接口的阻塞或解除阻塞。在正常状态下，RPL Owner 阻塞其 RPL 接口以防止业务形成环路。
- RPL Neighbor：与 RPL 相连的另一个环网节点称为 RPL Neighbor，配合 RPL Owner 完成保护倒换。
- 协议 VLAN：协议 VLAN 是 G.8032 采用的用于承载 R-APS 报文的独立 VLAN 通道。
- 阻塞 VLAN：业务 VLAN，不同于协议 VLAN 承载 R-APS 报文，是进行业务信息传递的 VLAN。
- R-APS 消息：定义在 G.8032 标准中的快速倒换协议报文。包括如下消息类型：
  - FS（Forced Switching）：FS 节点定期发送的消息用于执行强制倒换。
  - SF（Signal Failed）：故障节点定期发送的消息用于上报故障消息。
  - MS（Manual Switching）：MS 节点定期发送的消息用于执行手工倒换。
  - NR，RB（No Request Request Block）：RPL Owner 节点在无故障和无手动命令情况下定期发送通知环上其他节点的消息；用于 RPL Owner 节点阻塞 RPL 后定期发送此消息。
  - NR（No Request）：用于故障或管理命令清除时发送的消息。

在环网保护过程中，会使用 Guard Timer、WTR（Wait To Restore，等待恢复） Timer、WTB（Wait To Block，等待阻塞）Timer 和 Holdoff Timer 四个定时器。

- Guard Timer：用于过滤掉无效的 R-APS 报文，避免环上接收到无效的 R-APS 报文而产生的环上节点的错误保护倒换动作。尤其是在较大的环网络中，节点故障后如果立即恢复，可能会收到从环上传来的邻居节点发送的故障通知，从而再次

陷于 Down 状态，而这个通知却是由本节点引起的。配置环 Guard Timer 可以解决这个问题。

- WTR Timer：当工作路径恢复正常时，RPL Owner 上的 WTR Timer 开始计时。当 WTR Timer 计时器超时才恢复业务到工作路径。WTR Timer 用于避免工作路径不稳定而引起频繁倒换。
- WTB Timer：在返回模式下，当手动命令被清除时用于 RPL Owner 上延迟 RPL 端口阻塞的定时器，避免重复阻塞端口带来的震荡。
- Holdoff Timer：当检测到一个或多个新的故障后，如果设置的 Holdoff Timer 值不为 0，则启动 Holdoff Timer。在 Holdoff Timer 未超时时间内，系统会延时发送故障消息，即延时一段时间后再倒换到保护链路，可以防止链路震荡引起的频繁倒换。当 Holdoff Timer 超时，不论触发该定时器启动的这个故障是否仍然存在，都将检查链路状态，若存在故障则发送故障消息至保护倒换。

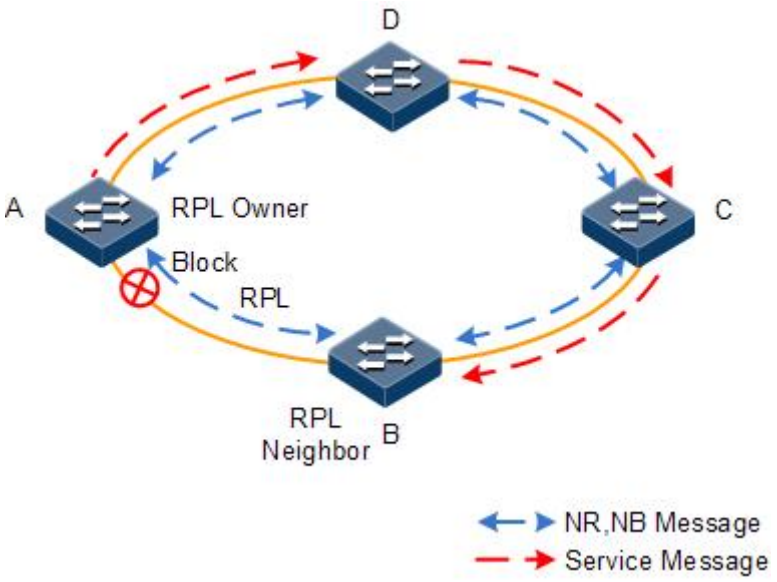
环状态

G.8032 定义了环网节点的 5 种状态。

- 空闲状态（Idle State）：无故障时的正常工作状态。
- 保护状态（Protecting State）：检测到链路故障后切换到的保护状态，该自动倒换过程由以太网 OAM（Operation, Administration and Maintenance，操作、管理与维护）的 CCM（Continuity Check Message，故障检测报文）检测到故障而触发。
- 挂起状态（Pending State）：故障修复前的悬而未决状态。
- 强制倒换状态（FS State）：下发强制倒换命令时的状态。
- 手工倒换状态（MS State）：下发手工倒换命令时的状态。

当系统无故障或故障恢复时，G.8032 以太网环处于空闲状态，空闲状态示意图如图 9-4 所示。

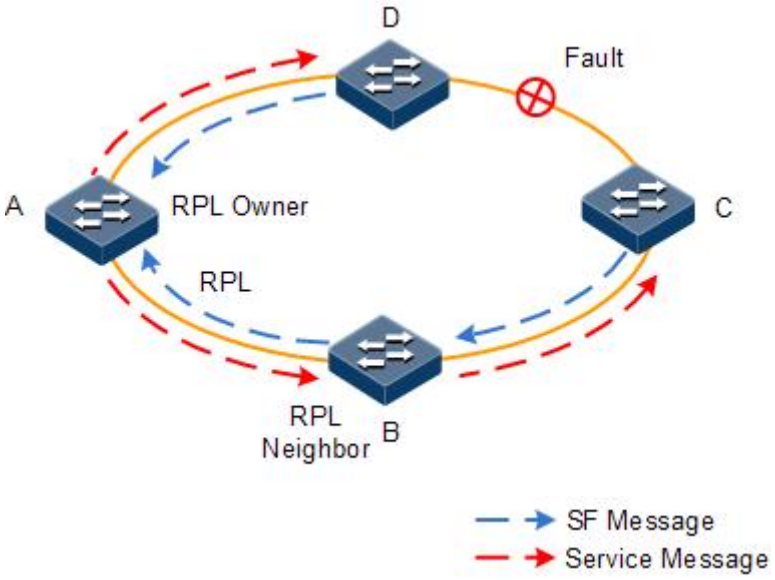
图 9-4 环网空闲状态



如图 9-4 所示，当环网处于空闲状态时，链路有如下的特征：

- 所有的节点在物理拓扑上以环的方式连接。
- G.8032 协议通过 RPL Owner 不断发送（NR，RB）信号，表示无故障，阻塞 RPL 链路，以确保不会成环。
- 相邻节点对每条链路使用以太网 OAM 中的 CCM 报文对链路进行监测。
- 当环路中出现故障时，G.8032 协议采用信号故障（SF）类型触发环路保护倒换。

图 9-5 环网保护状态



如图 9-5 所示当检测到环网故障时，启动自动保护倒换，进入保护状态：

- 在 Holdoff Timer 超时后，RPL Owner 触发与故障链路相邻的节点对故障链路进行阻塞，并发送 SF 信号向链路中其它节点报告该故障。如图 9-5 中的 C、D 节点间的故障发生后，D 节点和 C 节点分别向其它节点发送 SF 信号。
- SF 信号触发 RPL Owner 打开阻塞接口，并触发所有节点进行 FDB（Forwarding Database，转发数据库）清空，进入保护状态。

当故障恢复时，链路进行故障恢复倒换：

- 故障相邻的节点继续保持阻塞状态，Guard Timer 超时后，C、D 节点向其它节点发送 R-APS 的 NR 信号，表示没有本地故障请求。
- 当 RPL Owner 收到第一个 NR 信号后，立即启动 WTR Timer。
- 当 WTR 超时后，RPL Owner 阻塞 RPL，并发送 R-APS 的（NR，RB）信号，表示无本地故障请求，RPL 链路为阻塞状态。
- 其他节点收到该信号后，刷新 MAC 地址转发 FDB，发送 NR 信号的节点停止周期性发送报文，并打开原因故障阻塞的接口。
- 链路中各节点返回空闲状态。

子环

G.8032 的修订版增加了以太网多环的保护方案。子环是现存环网的附属环，通过互联节点（连接多个环的节点）与其它环或网络连接构成环。子环并不闭合，互联节点也不属于子环。

图 9-6 子环模型

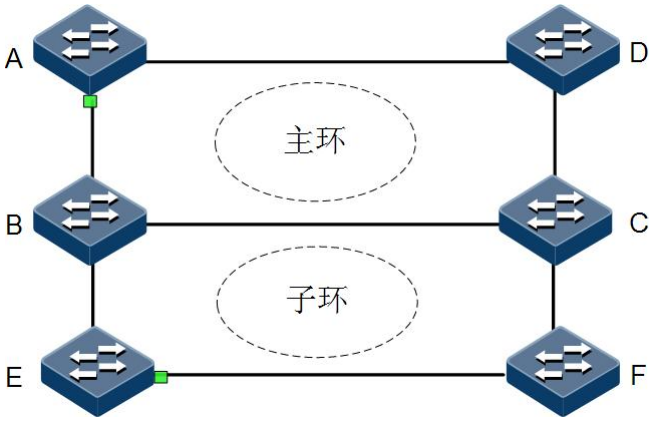


图 9-6 中，B 和 C 为互联节点，连接两个互联节点之间的通道称为 R-APS 虚通道，R-APS 虚通道用于相交环拓扑中的相交节点，如果相交环带有 R-APS 虚通道，则主环为子环 APS 报文提供虚拟通路，即子环 APS 报文会被传送到主环；如果不带，则主环不为子环提供虚拟通路，即子环 APS 报文在相交节点处被终结。主环和子环各自成环，每个环设定自己的 RPL Owner。多环的保护和单环类似，各自处理自己环内的故障。当互联节点间的共享链路出现故障时，主环切换到保护状态，子环不做处理。

因为子环的数据需要通过主环转发，所以主环设备上会存在子环的 MAC 地址列表，在子环出现故障时需要通过 Propagate 开关及时通知主环刷新 FDB，避免流量丢失。

环模式

返回模式与非返回模式的区别如下：

- 返回模式：等待 WTR 定时器超时后，流量切换到未发生故障前的链路进行转发。
- 非返回模式：等待 WTR 定时器超时后，流量不切换到未发生故障前的链路。缺省情况下，保护环处于返回模式。

子环的虚通路模式如下：

- **with** 模式：子环使用 R-APS 虚通道。主环为子环 APS 报文提供通路，子环相交节点收到子环 APS 报文会传送到主环，利用主环完成子环相交节点间的通信。
- **without** 模式：子环不使用 R-APS 虚通道。相交节点上子环 APS 报文要求终结，不会传送到主环。这种方式要求子环不能阻塞子环协议 VLAN（以保证子环报文可以通过 Owner）。

9.3.2 配置准备

场景

随着以太网向电信级网络的发展，语音、视频组播业务对以太网的冗余保护和故障恢复时间提出了更高的要求。现有的 STP 机制对故障恢复的收敛时间都在秒级，远远达不到要求。G.8032 技术通过定义环上节点的不同角色，在正常情况下阻断环路防止产生广播风暴，在环上链路或节点故障的情况下迅速切换到备份链路，从而实现消除环路、故障保护倒换和自动故障恢复等功能，并且故障保护倒换时间低于 50ms，支持单环、相交环和相切环三种组网方式。

G.8032 提供基于物理接口状态来检测故障，能够快速获知链路故障达到快速倒换的目的，适用于相邻设备之间。

前提

在配置 G.8032 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up；
- 创建 VLAN；
- 将接口加入 VLAN。

9.3.3 G.8032 的缺省配置

设备上 G.8032 的缺省配置如下。

功能	缺省值
保护环模式	返回模式
环 WTR 定时器	5min
环协议版本	2
Guard 定时器	500ms
环 HOLDOFF 定时器	0
相交节点上子环虚通路模式	with 模式
相交节点上环 Propagate 开关	禁止

9.3.4 创建 G.8032 保护环

注意

环上只允许一台设备配置为 RPL（Ring Protection Link，环保护链路）Owner，一台设备配置为 RPL Neighbour，其他设备只能配置为环转发节点。

相切环实际为两个独立的单环，配置与普通单环相同；相交环分为主环和子环，主环与单环配置相同，子环配置请参见“9.3.5 创建 G.8032 保护子环”。

ERPS 环接口需要工作在 switch 交换模式。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**g8032 instance** *instance-id*	创建 G8032 实例并进入配置节点
3	JX(config-g8032-instance-*)#**control-vlan** *vlan-id*	指定控制 vlan，如果配置了 **revertive dsiable**，则保护环变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由环保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护环处于返回模式。
4	JX(config-g8032-instance-*)#**data-vlan** *vlan-id*	指定数据 vlan
5	JX(config-g8032-instance-*)# **add interface** *interface-type interface-number* [**rpl** { **owner** | **neighbor** }]	配置端口并指定 rpl 角色
9	JX(config-g8032-instance-*)#**version** { **v1** | **v2** }	配置协议版本。同一个环上所有节点协议版本应一致，版本 1 通过协议 VLAN 区分不同环，因此不同环需配置不同的协议 VLAN，即使使用协议版本 2 也建议不同环配置不同的协议 VLAN。
10	JX(config-g8032-instance-*)#**guard-timer** *guard-time*	配置环 Guard 定时器后，到时之前的时间内不转发收到的任何协议报文。在节点发生恢复事件时 guard 定时器启动。在较大的环网络中，节点故障后如果立即恢复，可能会收到从环上传来的邻居节点发送的过时的故障通知，从而再次陷于 Down 状态，而这个通知却是由本节点引起的。
11	JX(config-g8032-instance-*)#**wtr-timer** *wtr-time*	配置环 WTR 定时器。在返回模式下当工作链路故障恢复时，等待 WTR 定时器超时之后，才会恢复到工作链路上工作。

步骤	配置	说明
12	JX(config-g8032-instance-*)#**holdoff-timer** *holdoff-time*	配置环 HOLDOFF 定时器后，当工作链路故障时，系统会延时上报故障，即延时一段时间后再倒换到保护链路，可以防止工作链路震荡引起的频繁倒换。 **说明** HOLDOFF 定时器配置值较大时会影响 50ms 倒换性能，所以推荐使用缺省值 0。

9.3.5 创建 G.8032 保护子环

注意

- 只有相交环存在主环和子环之分。
- 相交环主环的配置与单环或相切环相同，具体配置请参见“创建 G.8032 保护环”。
- 配置相交环时应先配置主环，再配置子环，否则子环找不到主环接口，将无法建立子环虚通路。
- 子环的实例号必须大于主环的实例号。
- 相交环子环上的非相交节点配置与单环或相切环相同，具体配置请参见“9.3.4 创建 G.8032 保护环”。
- ERPS 环接口需要工作在 switch 交换模式。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)# **g8032 instance** *instance-id*	创建实例

步骤	配置	说明
3	JX(config-g8032-instance-*)#**control-vlan** *vlan-id*	指定控制 vlan，如果配置了 **revertive dsiable**，则保护环变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由环保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护环处于返回模式。 **说明** 相交环两个相交节点之间的链路属于主环，所以在相交节点上配置子环时只能配置 port1 或 port2，不能同时配置。
4	JX(config-g8032-instance-*)#**data-vlan** *vlan-id*	指定数据 vlan
5	JX(config-g8032-instance-*)#**virtual-control-vlan** *vlan-id*	指定虚通道 vlan
6	JX(config-g8032-instance-*)# **add interface** *interface-type interface-number* [**rpl** { **owner** | **neighbor** }]	配置端口并指定 rpl 角色
7	JX(config-g8032-instance-*)# **add interface ge 1/0/1 vc-mep**	配置端口并指定为 vc-mep。 在相切环中，公共链路已经被主环占用，子环无法利用公共链路收发包，vc-mep 端口用于子环实例通过虚拟端口发包到公共链路的另一端。Vc-mep 端口在公共链路的两台设备上配置，配置成非公共链路的子环端口。

9.3.6 配置 G.8032 倒换控制

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config-g8032-instance-*)#**force-switch** *interface-type interface-number*	配置环上的流量强制倒换。 强制倒换可配置在多个环节点的多个接口上。
3	JX(config-g8032-instance-*)#**manual-switch** *nterface-type interface-number*	配置环上的流量手工倒换，优先级低于强制倒换和工作链路故障时产生的自动倒换。 手工倒换只能配置在同一个环节点的一个接口上。

说明

缺省情况下，工作链路故障时流量会自动倒换到保护链路。所以只在某些特殊情况下才需要配置 ERPS 倒换控制。

9.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show g8032 interface**	查看 G.8032 环接口状态信息。
2	JX#**show g8032 instance**	查看 G.8032 环状态信息。

9.3.8 维护

用户可以通过以下命令，维护设备 ERPS 特性的运行情况和配置情况。

命令	描述
JX(config-g8032-instance-*)#**clear**	清除环倒换控制命令（force-switch、manual-switch、WTR 定时器超时和 WTB 定时器超时）的作用。

9.3.9 配置单环 G.8032 保护示例

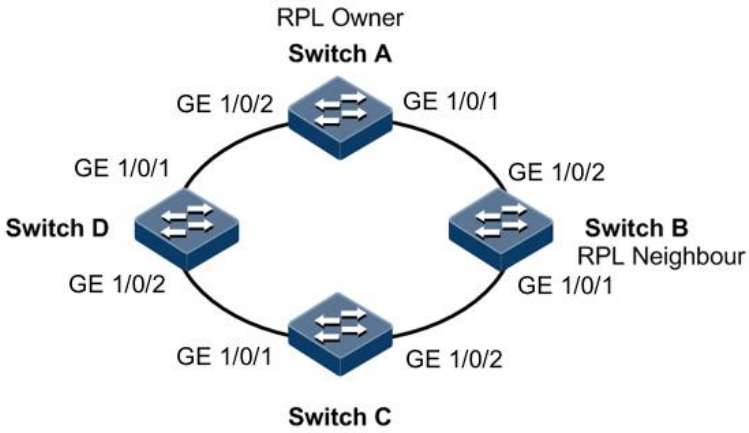
组网需求

如所示，为提高以太网络的可靠性，Switch A、Switch B、Switch C 和 Switch D 四台设备组成 G.8032 单环。

Switch A 设备作为 RPLOwner，Switch B 为 RPL Neighbour，Switch A 和 Switch B 之间的 RPL 链路阻塞。

协议控制 VLAN 为 1，阻塞的 VLAN 范围为缺省值 2～10。

图 9-7 单环 G.8032 应用组网示意图



配置步骤

步骤 1 配置接口加入 VLAN 2～VLAN 10。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#interface ge 1/0/1 to GE 1/0/2
SwitchA(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan 2-10
SwitchA(config-ge-1/0/1->ge-1/0/2)#exit
```

Switch B，Switch C，Switch D 配置同 Switch A

步骤 2 创建 ERPS 保护环。

配置 Switch A。

```
SwitchA(config)#g8032 instance 1
SwitchA(config-g8032-instance-1)#control-vlan 1
SwitchA(config-g8032-instance-1)#data-vlan 2-10
SwitchA(config-g8032-instance-1)#add interface ge 1/0/1 rpl owner
SwitchA(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch B。

```
SwitchB(config)#g8032 instance 1
SwitchB(config-g8032-instance-1)#control-vlan 1
SwitchB(config-g8032-instance-1)#data-vlan 2-10
SwitchA(config-g8032-instance-1)#add interface ge 1/0/1 rpl neighbor
```

```
SwitchA(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch C。

```
SwitchC(config)#g8032 instance 1
SwitchC(config-g8032-instance-1)#control-vlan 1
SwitchC(config-g8032-instance-1)#data-vlan 2-10
SwitchC(config-g8032-instance-1)#add interface ge 1/0/1
SwitchC(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch D。

```
SwitchD(config)#g8032 instance 1
SwitchD(config-g8032-instance-1)#control-vlan 1
SwitchD(config-g8032-instance-1)#data-vlan 2-10
SwitchD(config-g8032-instance-1)#add interface ge 1/0/1
SwitchD(config-g8032-instance-1)#add interface ge 1/0/2
```

检查结果

在设备上通过 **show g8032 interface** 查看 G.8032 保护环是否生效。

以 Switch A 为例，RPL 链路被阻断防止环路产生，WTR 定时器超时后环状态信息如下：

```
SwitchA#show g8032 interface

Instance Interface      Role    Type    Operate   Forward    Rx-Count  Tx-
Count

-------------------------------------------------------------------------
---------------------------
1       ge 1/0/1        port1   rpl     working   blocking   0         15
1       ge 1/0/2        port2   normal  working   forwarding 0         11
-------------------------------------------------------------------------
---------------------------
```

手动断开 Switch B 和 Switch C 之间的链路模拟故障，在 Switch A 上再次使用命令查看 G.8032 保护环状态，RPL 链路切换为转发状态。

```
SwitchA#show g8032 interface
Instance Interface      Role    Type    Operate   Forward    Rx-Count  Tx-
Count
-------------------------------------------------------------------------
---------------------------
1       ge 1/0/1        port1   rpl     working   forwarding 16        41
1       ge 1/0/2        port2   normal  failed    blocking   18        42
-------------------------------------------------------------------------
---------------------------
```

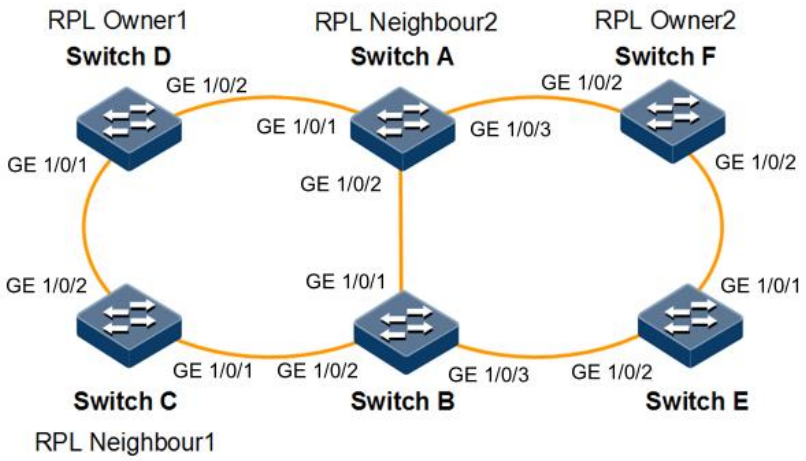
9.3.10 配置相交环 G.8032 保护示例

组网需求

如图 9-8 所示，为提高以太网络的可靠性，Switch A、Switch B、Switch C、Switch D、Switch E 和 Switch F 六台设备以 ERPS 相交环的形式组网。

- Switch A、Switch B、Switch C 和 Switch D 组成主环，Switch D 为主环 RPL Owner，Switch C 为主环 RPL Neighbour，阻断端口为 Switch D 的 GE 1/0/1，协议控制 VLAN 采用 VLAN 1。
- Switch A、Switch B、Switch E 和 Switch F 组成子环，Switch F 为子环 RPL Owner，Switch A 为子环 RPL Neighbour，阻断端口为 Switch F 的 GE 1/0/1，协议控制 VLAN 为 VLAN 4094。
- 主环和子环的阻塞 VLAN 范围均为缺省的 1～4094。

图 9-8 相交环 G.8032 应用组网示意图



配置步骤

步骤 1 创建 VLAN，并配置接口加入 VLAN。

配置 Switch A & B。

```
Switch#configure
Switch(config)#vlan 1-4094
Switch(config)#interface ge 1/0/1 to GE 1/0/3
Switch(config-ge-1/0/1->ge-1/0/3)#port link-type trunk
Switch(config-ge-1/0/1->ge-1/0/3)#port trunk allow-pass vlan all
Switch(config-ge-1/0/1->ge-1/0/3)#exit
```

配置 Switch C & D & E & F。

```
Switch#configure
Switch(config)#vlan 1-4094
Switch(config)#interface ge 1/0/1 to GE 1/0/2
Switch(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
Switch(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan all
Switch(config-ge-1/0/1->ge-1/0/2)#exit
```

步骤 2 创建 G.8032 保护环主环。

配置 Switch A & B。

```
Switch(config)#g8032 instance 1
```

```
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1
Switch(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch C。

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1
Switch(config-g8032-instance-1)#add interface ge 1/0/2 rpl neighbour
```

配置 Switch D。

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1 rpl owner
Switch(config-g8032-instance-1)#add interface ge 1/0/2
```

步骤 3 配置 G.8032 保护环子环。

配置 Switch A。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/3 rpl owner
Switch(config-g8032-instance-2)#virtual-control-vlan 3
Switch(config-g8032-instance-2)#add interface ge 1/0/3 vc-mep
```

配置 Switch B。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/3
Switch(config-g8032-instance-2)virtual-control-vlan 3
Switch(config-g8032-instance-2)#add interface ge 1/0/3 vc-mep
```

配置 Switch E。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/1
Switch(config-g8032-instance-2)#add interface ge 1/0/2
```

配置 Switch F。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/1 rpl neighbour
Switch(config-g8032-instance-2)#add interface ge 1/0/2
```

检查结果

在设备上通过 **show g8032 interface** 查看 G.8032 保护环是否生效。

分别在 Switch A、Switch D 和 Switch F 上检查，等待 WTR 定时器超时后，结果如下。

```
SwitchD#show g8032 interface

Instance Interface      Role   Type   Operate   Forward    Rx-Count  Tx-
Count

-------------------------------------------------------------------------
--------------------------
1       ge 1/0/1       port1   rpl    working   blocking   0        15
1       ge 1/0/2       port2   normal  working   forwarding  0        11
-------------------------------------------------------------------------
--------------------------
```

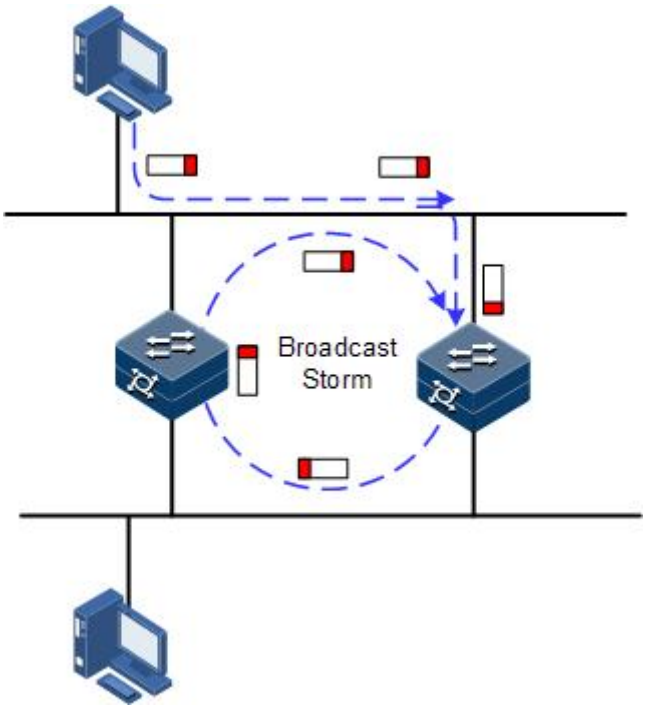
9.4 STP/RSTP

9.4.1 简介

STP

随着网络结构的日益复杂和网络中交换机数量的增多，网络环路成为以太网中最突出的问题。由于交换机对报文的广播机制，网络环路会使得网络中产生网络风暴，耗尽网络资源，对正常的数据转发产生严重的影响。由于网络环路产生的网络风暴示意图如下图所示。

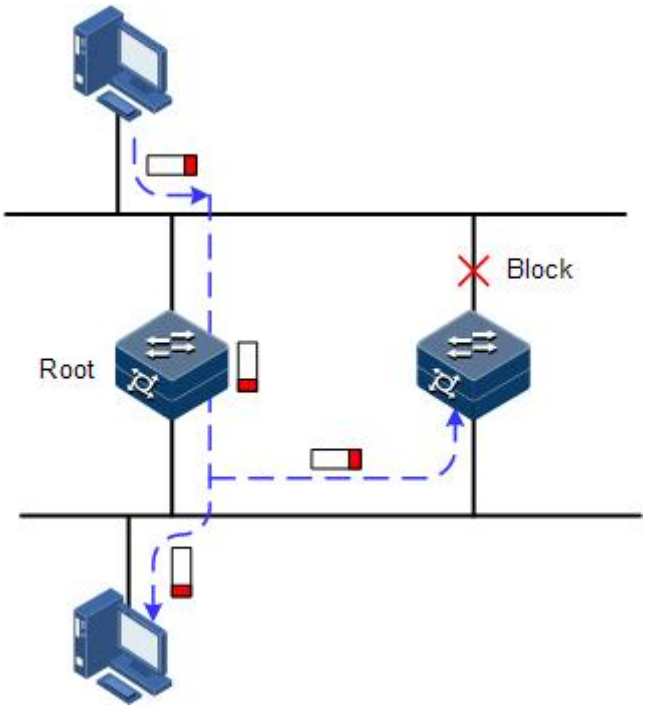
图 9-9 网络环路造成网络风暴示意图



STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1d 标准建立的，用于在局域网中消除数据链路层物理环路的协议。

运行 STP 的设备可以通过彼此交互 BPDU（Bridge Protocol Data Unit，桥协议数据单元）报文进行根交换机的选举、根端口和指定端口的选择，并根据选择结果对设备中存在环路的接口进行逻辑上的阻塞，最终将环路网络结构修剪成以某一台设备为根（Root）的无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环而导致广播风暴，并避免主机由于重复接收相同的报文造成的报文处理能力下降的问题发生。运行了 STP 协议的环网示意图如下图所示。

图 9-10 运行 STP 协议的环网示意图



虽然 STP 协议能够很好的消除环网，防止广播风暴的产生，但是随着应用的深入和网络技术的发展，STP 协议的缺点也逐渐暴露了出来。

STP 协议的主要缺点表现在收敛速度较慢。

RSTP

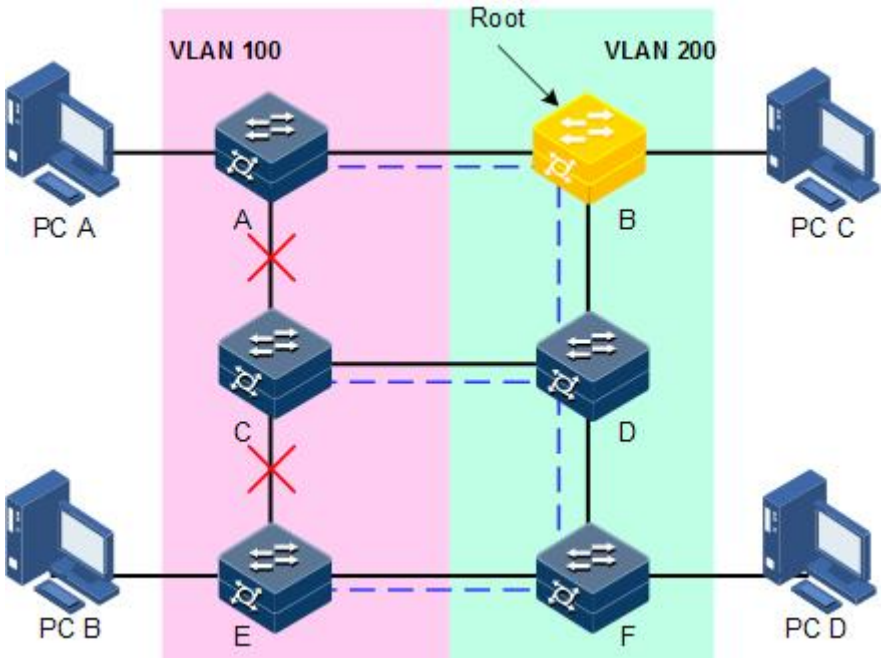
为了弥补 STP 协议收敛速度较慢的不足，IEEE 802.1w 制定了 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）。在普通 STP 协议的基础上，增加了接口可以快速由阻塞状态转变为转发状态的机制，加快了拓扑的收敛速度。

STP/RSTP 协议的目的都是将一个桥接的局域网，修剪成为逻辑拓扑上的一棵单一的生成树，从而避免广播风暴的产生。

由于 VLAN 技术快速发展，STP/RSTP 的局限性逐渐暴露出来。STP/RSTP 协议将网络拓扑修剪为单一生成树，会导致以下问题：

- 整个交换网络只有一个生成树，在网络规模比较大的时候会导致较长的收敛时间。
- 链路被阻塞后将不承载任何流量，造成带宽的浪费。
- 在网络结构不对称时，可能造成部分 VLAN 的报文无法转发。如下图所示，由于 RSTP 协议，选举 Switch B 为根交换机，且逻辑上阻断了 Switch A 和 Switch C 之间的链路，造成 VLAN 100 中的 VLAN 报文无法转发，Switch A 和 Switch C 无法通信。

图 9-11 RSTP 协议造成 VLAN 报文无法转发示意图



9.4.2 配置准备

场景

在较大型的局域网中，有多台设备进行级连满足多主机相互访问的需求，为防止设备之间组成环路造成 MAC 地址学习错误，并导致数据帧快速在环路中进行复制转发造成广播风暴、网络瘫痪，需要在这些设备上开启 STP。通过 STP 协议计算，阻塞掉环路当中的其中一个接口，保证每一个数据流去往目的主机的路径只有一条，并且被 STP 协议计算为最优路径。

前提

无

9.4.3 STP 的缺省配置

设备上 STP 的缺省配置如下。

功能	缺省值
全局 STP 功能状态	禁止
接口 STP 功能状态	使能
设备的 STP 优先级	32768
接口的 STP 优先级	128

功能	缺省值
接口的路径开销	0
Max Age 定时器	20s
Hello Time 定时器	2s
Forward Delay 定时器	15s

9.4.4 使能 STP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**stp mode** { **stp** | **rstp** | **mstp** | **default** }	配置生成树的运行模式。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
4	JX(config-ge-1/0/*)#**stp enable**	使能接口生成树协议。

9.4.5 配置 STP 参数

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp priority** *priority-value*	配置设备优先级。
3	JX(config)#**interface** *interface-type interface-number* JX(config-ge-1/0/*)#stp **priority** *priority-value*	配置设备接口优先级。
4	JX(config-ge-1/0/*)#**stp path-cost** *cost-value*	配置设备接口路径开销。
5	JX(config)#**stp hello-time** *value*	配置 Hello Time 的值。
6	JX(config)#**stp forward-delay** *value*	配置 Forward Delay 的值。
7	JX(config)#**stp max-age** *value*	配置 Max Age 的值。
8	JX(config)#**stp pathcost-standard** { **dot1d-1998** | **dot1t** }	配置生成树路径开销计算标准。

9.4.6 配置 RSTP 边缘接口

边缘接口是指不直接与任何设备连接，也不通过接口所连接的网络间接与任何设备相连的接口。

设置为边缘接口能够使该接口的状态迅速转变为转发状态，而不需要时间等待，对于直接与用户终端相连的以太网接口，为能使其快速迁移到转发状态，应将其设置为边缘接口。

当某个接口设置为边缘接口（enable）时，当接口收到 BPDU 后实际运行值会变为非边缘接口。当某个接口设置为非边缘接口（disable）时，同样，无论其实际情况下为边缘或非边缘接口，此接口会保持为非边缘接口，直到配置改变。

缺省情况下，以太网设备中所有接口的均设置为 disable。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp edge-port** { **enable** | **disable** }	配置 RSTP 边缘接口属性。

9.4.7 配置 RSTP 链路类型

点对点链路相连的两个接口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，根据双工状态设定接口的链路类型。全双工接口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网接口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现接口是否与点到点链路相连。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp point-to-point** { **force-true** | **force-false** | **auto** }	配置接口的链路类型。

9.4.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

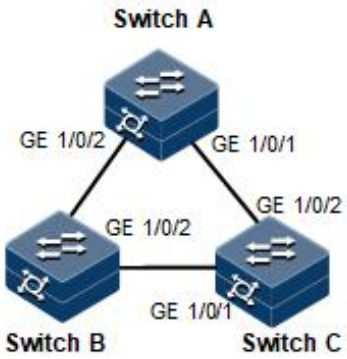
序号	检查项	说明
1	JX#show stp infomation	查看 STP 基本配置信息。
2	JX#show stp interface	查看接口下生成树配置信息。
3	JX#show stp bridge	查看 stp 根桥信息

9.4.9 配置 STP 示例

组网需求

如下图所示，三台设备 Switch A、Switch B 和 Switch C 组网成一个环，需在物理链路成环情况下解决环路问题，三台设备上需开启 STP，并设置 Switch A 的优先级为 0，Switch B 到 Switch A 的开销改为 10。

图 9-12 STP 应用组网示意图



配置步骤

步骤 1 在三台设备上均开启 STP 功能。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#stp mode stp
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#configure
```

```
SwitchB(config)#stp mode stp
```

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#configure
SwitchC(config)#stp mode stp
```

步骤 2 配置三台设备的接口模式。

配置 Switch A。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#stp enable
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#stp enable
SwitchA(config-ge-1/0/2)#exit
```

配置 Switch B。

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#stp enable
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#port link-type trunk
SwitchB(config-ge-1/0/2)#stp enable
SwitchB(config-ge-1/0/2)#exit
```

配置 Switch C。

```
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#port link-type trunk
SwitchC(config-ge-1/0/1)#stp enable
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#port link-type trunk
SwitchC(config-ge-1/0/2)#stp enable
SwitchC(config-ge-1/0/2)#exit
```

步骤 3 配置生成树优先级及接口路径开销。

配置 Switch A。

```
SwitchA(config)#stp priority 0
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#stp path-cost 10
```

配置 Switch B。

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#stp path-cost 10
```

检查结果

通过 **show stp** 命令查看桥状态，以 Switch A 为例。

```
SwitchA#show stp infomation
--------------------------------------------------------------------------
-------
  Mode                              : stp
  Trap state                         : disable
  Bridge type                        : customer
  BPDU Guard state                    : disable
  TC protection state                  : disable
  TC protection threshold               : 2
  Hello time                         : 2
  Max age                           : 20
  Forward delay                      : 15
  Max hops                          : 20
  Time factor                        : 6
  Format selector                     : 0
  Revision level                     : 0
  Config name                       : region
  TC flush arp state                   : disable
  Migration time                     : 3
  Pathcost standard                   : dot1t
  TC holdoff time                    : 10
  Transmit limit                     : 6 (packets/s)
  Link detection state                 : enable
  Edge default state                  : disable
--------------------------------------------------------------------------
-------
```

通过 **show stp interface** 查看接口状态，以 Switch A 为例。

```
SwitchA#show stp interface
  MSTID Port         Role         State        Protection    Region
--------------------------------------------------------------------------
------------
  0    ge-1/0/1      designated    forward       --          different
  0    ge-1/0/2      designated    forward       --          different
```

9.5 MSTP

9.5.1 简介

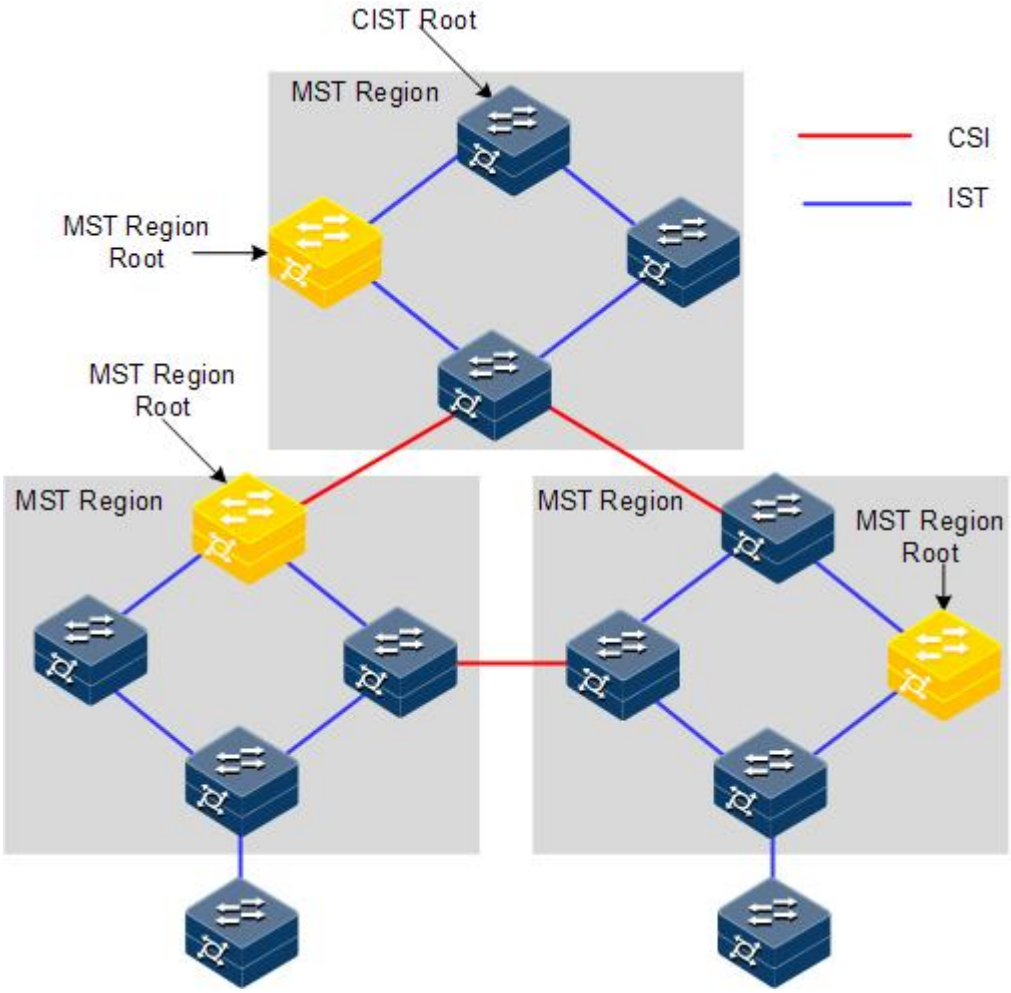
IEEE 802.1s 标准定义了 MSTP（Multiple Spanning Tree Protocol，多生成树协议）。MSTP 可以弥补 STP 和 RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而提供了很好的负荷分担机制。

MSTP 把一个交换网络划分成多个域，每个域叫做一个 MST 域。每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个 MSTI（Multiple Spanning Tree Instance，多生成树实例）。

MSTP 协议引入了 CST（Common Spanning Tree，公共生成树）和 IST（Internal Spanning Tree，内部生成树）的概念。其中 CST 是指把 MST 域当成一个整体时，计算生成的一棵生成树。而 IST 是指在 MST 域内部生成的生成树。

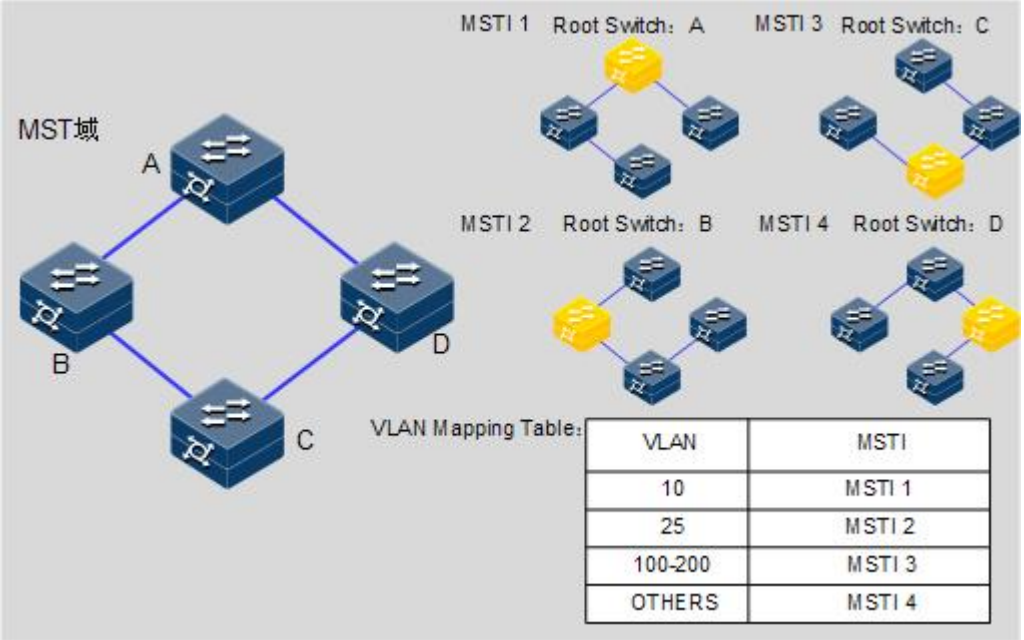
与 STP 和 RSTP 相比，MSTP 中还引入了总根（CIST Root）和域根（MST Region Root）的概念。总根是一个全局概念，对于所有运行的 STP/RSTP/MSTP 的交换机只能有 1 个总根，也即是 CIST 的根。而域根是一个局部概念，是相对于某个域的某个实例而言。如下图所示，所有相连的设备，总根只有 1 个，而每个域包含的域根数目与实例个数相关。

图 9-13 MSTP 网络基本概念示意图



在每个 MST 域中，可以有不同的 MST 实例，通过设置 VLAN 映射表（即 VLAN 和 MSTI 的对应关系表），把 VLAN 和 MSTI 联系起来。MSTI 概念示意图如下图所示。

图 9-14 MSTI 概念示意图

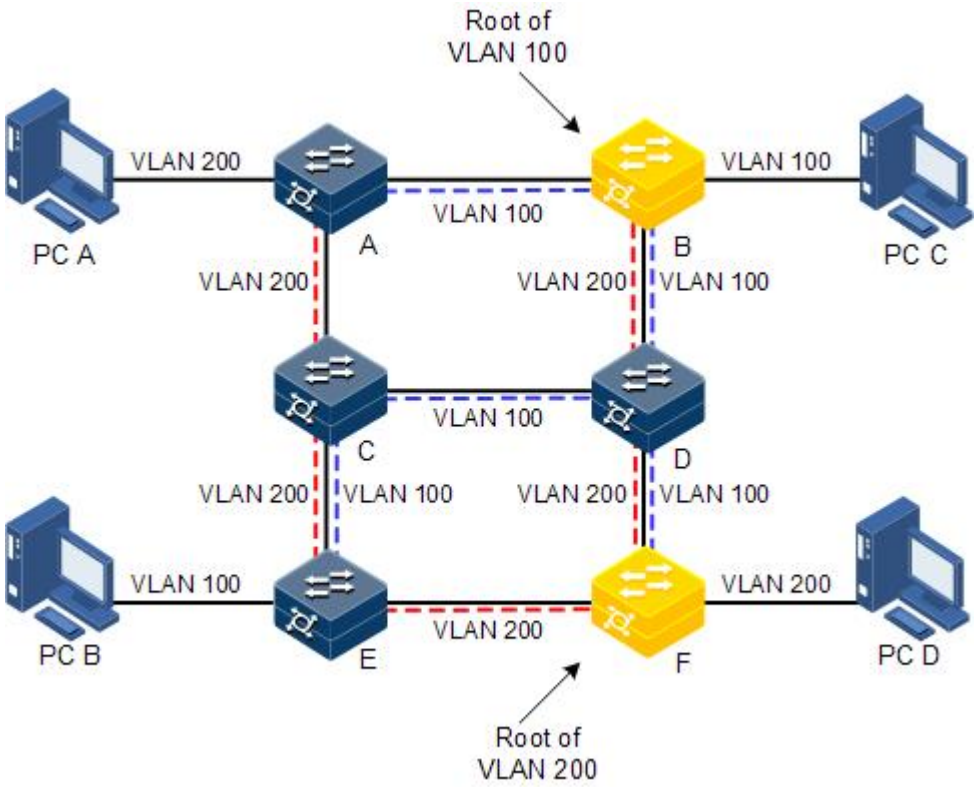


说明

每个 VLAN 只能对应一个 MSTI，即同一 VLAN 的数据只能在一个 MSTI 中传输；而一个 MSTI 可能对应多个 VLAN。

MSTP 协议相对于之前的 STP 协议和 RSTP 协议，优势非常明显。MSTP 具有 VLAN 认知能力，可以实现负载均衡分担，可以实现类似 RSTP 的端口状态快速切换，可以捆绑多个 VLAN 到一个 MST 实例中，以降低资源占用率。此外，网络中运行 MSTP 协议的设备可以很好的与运行 STP 协议和 RSTP 协议的设备兼容。

图 9-15 MST 域内多生成树实例组网示意图



将 MSTP 应用于如上图所示的网络，经计算最终生成两棵生成树（也即 2 个 MST 实例）：

- MSTI1 以 B 为根交换设备，转发 VLAN100 的报文；
- MSTI2 以 F 为根交换设备，转发 VLAN200 的报文。

这样所有 VLAN 内部可以互通，同时不同 VLAN 的报文沿不同的路径转发，实现了负荷分担。

9.5.2 配置准备

场景

大型局域网或小区汇聚时，汇聚设备之间组成一个环作为线路的备份，在实现线路备份的同时，需要防止环路以及实现业务的负载分担，MSTP 协议可以为每一个或一组 VLAN 选择不同且唯一的转发路径。

前提

无

9.5.3 MSTP 的缺省配置

设备上 MSTP 的缺省配置如下。

功能	缺省值
全局 MSTP 功能状态	禁止
接口 MSTP 功能状态	使能
MST 域的最大跳数	20
设备的 MSTP 优先级	32768
接口的 MSTP 优先级	128
接口的路径开销	0
每个 Hello time 内的最大发送报文数量	3
Max Age 定时器	20s
Hello Time 定时器	2s
Forward Delay 定时器	15s
MST 域的修订级别	0
TC 保护	禁用
TC 保护功能的阈值	1

9.5.4 使能 MSTP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**stp mode mstp**	配置生成树模式为 MSTP。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
4	JX(config-ge-1/0/*)#**stp enable**	使能接口生成树协议。

9.5.5 配置 MST 域和 MST 域最大跳数

当设备的运行模式为 MSTP 时，可为设备设置其归属的域信息。设备属于哪个 MST 域，是由域名，VLAN 映射表，MSTP 修订级别配置决定的。用户可以通过下面的配置过程将当前设备划分在一个特定的 MST 域内。

MST 域的最大跳数限制了 MST 域的规模。从域内的生成树的根桥开始，域内的配置消息（BPDU）每经过一台设备的转发跳数就被减 1，设备将丢弃收到的跳数为 0 的配置消息。使处于最大跳数外的设备无法参与生成树的计算，从而限制了 MST 域的规模。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp instance** *instance-id* **vlan** *vlan-list*	配置 MST 域的 VLAN 到实例映射关系。
3	JX(config)#**stp config-name** *name*	配置 MST 域名。
4	JX(config)#**stp revision-level** *level-value*	配置 MST 域的修订级别。
6	JX(config)#**stp max-hops** *hops-value*	配置设备 MST 域最大跳数。

说明

当且仅当配置的设备为域根时，配置的最大跳数才作为 MST 域的最大跳数，其他非域根桥配置此项无效。

9.5.6 配置设备接口和系统的优先级

接口是否被选为根接口需要根据接口优先级进行判断。同等条件下，接口优先级值越小，接口越优先被选为根接口。接口可在不同的实例中具有不同的接口优先级，也可以在不同实例中充当不同的角色。

设备 Bridge ID 的大小决定了这台设备是否能够被选作生成树的根。通过配置较小的优先级，可以得到较小的设备 Bridge ID，达到指定某台设备成为生成树树根的目的。优先级相同的情况下，MAC 地址小的为树根。

与配置根与备份根相同，优先级在不同实例中的配置相互独立。用户可以通过参数 **instance** *instance-id* 确定的配置优先级的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，则是为 CIST 配置的桥优先级。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。

步骤	配置	说明
3	JX(config-ge-1/0/*)#**stp** [**instance** *instance-id*] **priority** *priority-value* JX(config-ge-1/0/*)#**exit**	配置某个生成树实例的接口优先级。
4	JX(config)#**stp** [**instance** *instance-id*] **priority** *priority-value*	配置某个生成树实例的系统优先级。

优先级取值必须为 4096 的倍数，如 0、4096、8192 等，缺省值为 32768。

9.5.7 配置接口的路径开销

在选举根接口（root port）和指定接口（designated port）时，路径开销越小的接口越容易被选举为根接口或者指定接口。接口的路径开销在不同实例中的配置相互独立。用户可以通过参数 **instance** *instance-id* 确定的配置接口的内部路径开销的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，则是为 CIST 配置的接口内部路径开销。

接口的开销一般依据其物理特性，缺省情况如下：

- 10Mbit/s 为 2000000
- 100Mbit/s 为 200000
- 1000Mbit/s 为 20000
- 10Gbit/s 为 2000

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp** [**instance** *instance-id*] **path-cost** *cost-value*	配置接口的路径开销。

9.5.8 配置接口最大发送速率

MSTP 每 Hello Time 时间内允许发送的最大 BPDU 数量。此参数是一个相对值，没有单位，该参数被配置得越大，则每个 Hello Time 内允许发送的报文个数就越多，同时也会占用会更多的设备资源。与时间参数相同，只有根设备的此项配置生效。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**stp transmit-limit** *value*	配置接口最大发送速率。

9.5.9 配置 MSTP 定时器

- Hello Time：设备定期发送桥配置信息（BPDU）的时间间隔，用于设备检测链路是否存在故障。设备每隔 Hello Time 时间，会向周围的设备发送 Hello 报文，以确认链路是否存在故障。缺省值为 2s，用户可以根据网络情况对此值进行调整。当网络中链路出现频繁变化时，可以适当缩短该值，来增强生成树协议的健壮性。相反，增大此值则可以降低生成树协议对系统 CPU 资源的占用率。
- Forward Delay：保证设备状态安全迁移的时间参数。链路故障会引发网络重新进行生成树的计算，不过重新计算得到的新配置消息无法立刻传遍整个网络。如果新选出的根接口和指定接口立刻开始数据转发，可能会造成暂时性的路径回环。为此协议采用了一种状态迁移的机制：根接口和指定接口重新开始数据转发之前，要经历一个中间状态（学习状态），中间状态经过 Forward Delay 时间的延时后，才能进入转发状态。这个延时保证了新的配置消息已经传遍整个网络。用户可以根据实际情况调整该值，当网络拓扑不频繁变化时可以将该值减小，反之增大。
- Max Age：生成树协议所使用的桥配置信息有生存周期，用来判断配置消息是否过时。设备会将过时的配置消息丢弃。当桥配置信息过期后，生成树协议将重新计算生成树。缺省值为 20s，该值过小会导致生成树重计算过于频繁，过大则会导致生成树协议不能及时适应网络拓扑结构的变化。

整个交换网络中所有的设备采用 CIST 根设备上的三个时间参数，因此只有在根设备上的配置生效。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**stp hello-time** *value*	配置 HelloTime 的值。
3	JX(config)#**stp forward-delay** *value*	配置 Forward Delay 的值。
4	JX(config)#**stp max-age** *value*	配置 MaxAge 的值。

9.5.10 配置边缘接口

边缘接口是指不直接与任何设备连接，也不通过接口所连接的网络间接与任何设备相连的接口。

设置为边缘接口能够使该接口的状态迅速转变为转发状态，而不需要时间等待，对于直接与用户终端相连的以太网接口，为能使其快速迁移到转发状态，应将其设置为边缘接口。

当某个接口设置为边缘接口自动检测（auto）则边缘接口的属性是由实际情况决定的。当某个接口设置为边缘接口（force-true）时，当接口收到 BPDU 后实际运行值会变为非边缘接口。当某个接口设置为非边缘接口（force-false）时，同样，无论其实际情况下为边缘或非边缘接口，此接口会保持为非边缘接口，直到配置改变。

缺省情况下，以太网设备中所有接口的均设置为自动检测属性。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp edge-port** { **enable** | **disable** }	配置接口边缘接口属性。

9.5.11 配置 BPDU 过滤

用户使能边缘接口的 BPDU 过滤功能后，边缘接口不会发送 BPDU 报文，也不会处理收到的 BPDU 报文。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#config**ure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp bpdu-filter {enable | disable}**	配置边缘接口的 BPDU 过滤功能。

9.5.12 配置 BPDU 保护

在交换机上，通常将直接与用户终端（如 PC 机）或文件服务器等非交换机设备相连的接口配置为边缘接口，以实现这些接口的快速迁移。

正常情况下，这些边缘接口不会收到 BPDU。如果有人伪造 BPDU 恶意攻击交换机，当这些接口接收到 BPDU 时，会自动将这些接口设置为非边缘接口，并重新进行生成树计算，从而引起网络震荡。

MSTP 提供 BPDU 保护功能来防止这种攻击。启动 BPDU 保护功能后，可以防止伪造 BPDU 恶意攻击。

如果使能 BPDU 保护功能，则边缘接口收到了 BPDU，设备将关闭这些接口，同时通知网管系统。被关闭的接口只能由网络管理人员通过命令手动恢复。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**stp bpdu-protection enable**	使能 BPDU 保护功能。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
4	JX(config-ge-1/0/*)#**stp bpdu-protection error-down recovery-interval** *interval*	配置 BPDU 保护的恢复周期

说明

当边缘接口使能了 BPDU 过滤功能，同时设备使能了 BPDU 保护功能，则 BPDU 保护功能优先生效，即边缘接口接收到 BPDU 报文时，接口被关闭。

9.5.13 配置 STP/RSTP/MSTP 模式切换

当生成树协议开启时，支持三种生成树运行模式，分别为 STP 兼容模式、RSTP 模式和 MSTP 模式。

- STP 兼容模式：不执行替换接口到根接口的快速转换和指定接口快速 Forwarding。只发送 STP 配置报文（STP Configuration BPDU）和拓扑变化通知（STP TCN BPDU）。收到 MST BPDU 将丢弃不识别部分。
- RSTP 模式：执行替换接口到根接口的快速转换和指定接口快速 Forwarding。只发送 RST BPDU。收到 MST BPDU 将丢弃不识别部分；如果本交换机接口的对端运行 STP 协议，接口将转移到 STP 兼容模式下。
- MSTP 模式：发送 MST BPDU。如果本交换机接口的对端运行 STP 协议，接口将转移到 STP 兼容模式下。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**stp mode { stp | rstp | mstp }**	配置生成树的运行模式。
3	JX(config-ge-1/0/*)#**stp mcheck**	(可选)强制端口变为 MSTP 模式。

9.5.14 配置链路类型

点对点链路相连的两个接口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，MSTP 根据双工状态设定接口的链路类型。全双工接口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网接口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现接口是否与点到点链路相连。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp point-to-point (force-true|force-false|auto)**	配置接口的链路类型。

9.5.15 配置根接口保护

当桥收到更高优先级的报文的时候就需要重新选举，重新选举一个是会影响网络的连通性，二来会消耗 CPU 资源。对于开启了 MSTP 功能的网络，如果有人发送高优先级的 BPDU 报文进行攻击，网络就会由于不断的选举而导致不稳定。而一般而言，各个桥的优先级是在网络规划阶段就已经配置好，越是靠近边缘的桥优先级越低，因此下行接口一般不会收到比桥优先级高的报文，除非有人恶意攻击。对于这些接口，可以通过开启根接口保护功能，拒绝处理比桥优先级高的报文，并在收到高优先级报文的时候阻塞接口一段时间，防止攻击源的其他攻击损害更上层的链路。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/*)#**stp root-protection enable**	使能接口的根接口保护功能。

9.5.16 配置接口环路保护

生成树主要作用有两个：防止环路和链路备份。防止环路就要求必须将拓扑裁剪成树状结构，而如果需要进行链路备份，拓扑中必须有冗余的链路。生成树就是通过阻塞

冗余链路来达到防止环路的功能，而在链路发生故障的时候放开冗余链路从而达到链路备份的功能。

生成树模块会周期性交换报文，如果一定时间内没有收到报文即认为发生了链路故障。然后选举，放开备份接口。而在实际应用中，导致收不到报文的原因可能并不是链路故障，如果在这种情况下放开备份接口就有可能导致环路。

环路保护的目的是当接口在一定时间内收不到报文的时候，不进行重新选举，保持接口原来的状态不变。注意：环路保护的功能和链路备份的功能是对立的，也即环路保护是以失去链路备份功能的代价来实现环路避免。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp loop-protection enable**	使能接口环路保护功能。

9.5.17 配置端口 TC 报文抑制功能

用户接入网络的拓扑改变会引起核心网络的转发地址更新，当用户接入网络的拓扑因某种原因而不稳定时，就会对核心网络形成冲击。为了避免这种情况，可以在端口上使能 TC 报文抑制功能，此后当该端口收到 TC 报文时，不会再向其他端口传播。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp tc-restriction enable**	配置端口 TC 抑制功能。

9.5.18 配置 TC 保护功能

TC 保护功能可避免拓扑变化相关的 BPDU 报文攻击，提高设备和网络的安全性。

- 使能 TC 保护功能后，在 STP 的 Hello Time 时间内，仅接收阈值数量以内的 TC 报文。该 Hello Time 时间内的、超过阈值数量的 TC 报文会被丢弃，直到下一个 Hello Time 时间再重新开始计算接收的 TC 报文数量。
- 禁用 TC 保护功能后，设备会处理所有 TC 报文。当设备受到 TC 报文攻击时，可能会导致业务中断、设备 CPU 利用率过高甚至无法正常工作。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**stp tc-protection threshold** *threshold-value*	配置 TC 保护功能的阈值。
3	JX(config)#**stp tc-protection enable**	配置 TC 保护功能。

9.5.19 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show stp infomation**	查看 STP 基本配置信息。
2	JX#**show stp interface**	查看接口下生成树配置信息。
3	JX#**show stp bridge**	查看 STP 根桥信息
4	JX#**show stp instance**	查看 STP 实例与 VLAN 映射关系。

9.5.20 维护

用户可以通过以下命令维护 MSTP 特性。

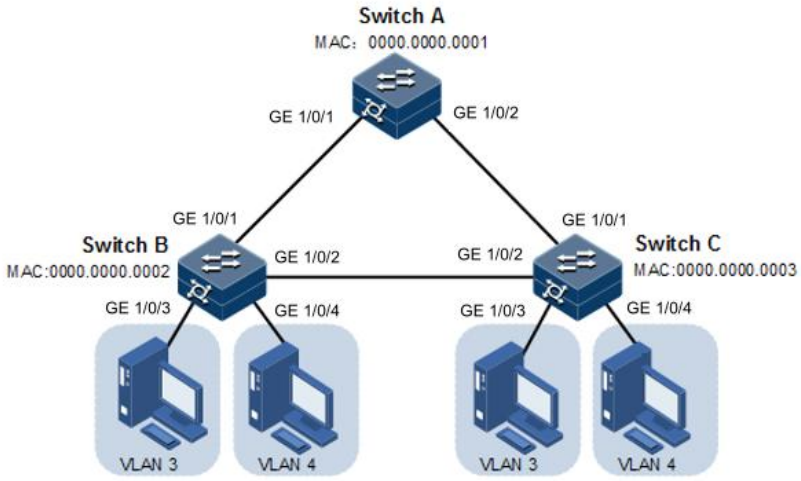
命令	描述
JX(config-ge-1/0/*)#**reset stp statistics**	清除接口生成树统计信息。

9.5.21 配置 MSTP 示例

组网需求

如下图所示，三台交换机设备组成环形网络运行 MSTP 协议，域名 aaa。Switch B 和 Switch C 上分别各连接两台 PC，分别属于 VLAN 3 和 VLAN 4。实例 3 关联 VLAN 3，实例 4 关联 VLAN 4。配置优先级，使得实例 3 的根桥为 Switch A，实例 4 的根桥为 SwicthB,这样可以使两个 VLAN 的报文分别在两条路径进行转发，消除了环路的同时实现了负载分担。

图 9-16 MSTP 应用组网示意图



配置步骤

步骤 1 在三台交换机上分别创建 VLAN 3 和 VLAN 4 并激活。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 3,4
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#configure
SwitchB(config)#vlan 3,4
```

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#configure
SwitchC(config)#vlan 3,4
```

步骤 2 Switch A 的接口 GE 1/0/1、GE 1/0/2 以 Trunk 模式允许所有 VLAN 通过，Switch B 的接口 GE 1/0/1、GE 1/0/2 以 Trunk 模式允许所有 VLAN 通过，Switch C 的接口 GE 1/0/1、GE 1/0/2 以 Trunk 模式允许所有 VLAN 通过。Switch B、Switch C 的接口 GE 1/0/3、GE 1/0/4 以 Access 模式分别允许 VLAN 3、VLAN 4 通过。

配置 Switch A。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
```

```
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/2)#exit
```

配置 Switch B。

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#port link-type trunk
SwitchB(config-ge-1/0/2)#port trunk allow-pass vlan all
SwitchB(config-ge-1/0/2)#exit
SwitchB(config)#interface ge 1/0/3
SwitchB(config-ge-1/0/3)#port link-type access
SwitchB(config-ge-1/0/3)#port default vlan 3
SwitchB(config-ge-1/0/3)#exit
SwitchB(config)#interface ge 1/0/4
SwitchB(config-ge-1/0/4)#port link-type access
SwitchB(config-ge-1/0/4)#port default vlan 4
SwitchB(config-ge-1/0/4)#exit
```

配置 Switch C。

```
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#port link-type trunk
SwitchC(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#port link-type trunk
SwitchC(config-ge-1/0/2)#port trunk allow-pass vlan all
SwitchC(config-ge-1/0/2)#exit
SwitchC(config)#interface ge 1/0/3
SwitchC(config-ge-1/0/3)#port link-type access
SwitchC(config-ge-1/0/3)#port default vlan 3
SwitchC(config)#interface ge 1/0/4
SwitchC(config-ge-1/0/4)#port link-type access
SwitchC(config-ge-1/0/4)#port default vlan 4
SwitchC(config-ge-1/0/4)#exit
```

步骤 3 Switch A、Switch B、Switch C 设置生成树模式为 MSTP，并开启生成树协议。进入 MSTP 配置模式设置域名为 aaa，修正版本为 0，instance 3 映射 VLAN 3、instance 4 映射 VLAN 4，退出 mst 配置模式。

配置 Switch A。

```
SwitchA(config)#stp mode mstp
SwitchA(config)#stp config-name aaa
SwitchA(config)#stp revision-level 0
SwitchA(config)#stp instance 3 vlan 3
SwitchA(config)#stp instance 4 vlan 4
SwitchA(config)#stp instance 3 priority 0
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#stp enable
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#stp enable
```

配置 Switch B。

```
SwitchB(config)#stp mode mstp
SwitchB(config)#stp config-name aaa
SwitchB(config)#stp revision-level 0
SwitchB(config)#stp instance 3 vlan 3
SwitchB(config)#stp instance 4 vlan 4
SwitchA(config)#stp instance 4 priority 0
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#stp enable
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#stp enable
```

配置 Switch C。

```
SwitchC(config)#stp mode mstp
SwitchC(config)#stp config-name aaa
SwitchC(config)#stp revision-level 0
SwitchC(config)#stp instance 3 vlan 3
SwitchC(config)#stp instance 4 vlan 4
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#stp enable
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#stp enable
```

步骤 4 Switch B 修改生成树实例 3 接口 GE 1/0/1 的开销为 500000。

```
SwitchB(config)#interface GE 1/0/1
SwitchB(config-ge-1/0/1)#stp instance 3 path-cost 500000
```

检查结果

通过 **show stp interface** 命令查看 MST 域的接口状态信息，以 Switch C 为例。

```
SwitchA#show stp interface
  MSTID Port         Role         State        Protection    Region
-------------------------------------------------------------------------------
------------
  0    ge-1/0/1      root         forward      --          same
  0    ge-1/0/2      alternate     discarding    --          same
  3    ge-1/0/1      root         forward      --          same
  3    ge-1/0/2      alternate     discarding    --          same
  4    ge-1/0/1      alternate     discarding    --          same
  4    ge-1/0/2      root         forward      --          same
-------------------------------------------------------------------------------
------------------------------
```

9.6 环路检测

9.6.1 简介

环路检测功能可以消除因环路对网络造成的影响，提高网络的自检错性、容错性和健壮性。

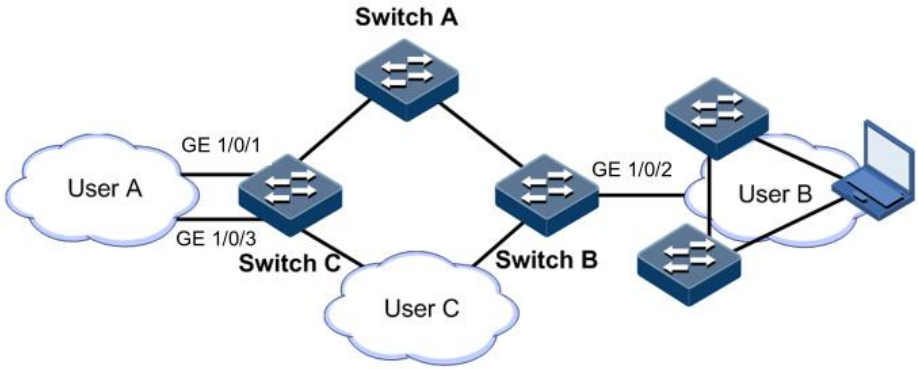
环路检测过程中每个开启环路检测功能的接口周期性地发送环路检测报文（Hello 报文），由于环路检测功能主要应用于网络边缘接口，因此，正常情况下边缘接口是不应该收到任何环路检测报文的。如果边缘设备接收到了环路检测报文，则认为网络出现了环路。接收环路检测报文分为两种情况：接收到了自身发送的报文和接收到了其他设备发送的报文，主要依据设备 MAC 地址和报文携带的 MAC 地址进行比较区分。

环路类型

常见的环路类型有自环、内环两种。如下图所示，Switch B 和 Switch C 是连接用户网络的边缘交换机。

- 自环：同一设备上同一以太网接口下存在的用户环路，例如用户网络 B 自身存在环路使 Switch B 的 GE 1/0/2 接口形成自环。
- 内环：同一设备上不同以太网接口之间形成的环路，例如 Switch C 的接口 GE 1/0/1 和接口 GE 1/0/3 与用户网络 A 形成内环。

图 9-17 环路类型示意图



环路处理机制

设备遵循如下原则进行环路处理：

- 如果接收和发送环路检测报文的设备是同一设备，但不是同一接口，则处理接口号小的接口消除环路（内环）。
- 如果接收和发送环路检测报文的设备是同一设备且是同一接口，则处理该接口消除环路（自环）。

在下图中，假设 Switch B 和 Switch C 连接用户网络的接口都使能了环路检测功能。环路检测针对不同环路类型的处理机制如下：

- 对于自环，Switch B 收发报文接口号相同，将在 GE 1/0/2 接口采取配置的环路检测动作来消除自环。
- 对于内环，Switch C 会收到自身发出的环路检测报文，而且收发报文接口号不同，因此会在接口号小的 GE 1/0/1 采取配置的环路检测动作来消除内环。

环路处理动作

环路处理动作即设备检测到接口出现环路时的处理方式，用户可以根据实际情况在指定接口上配置不同的环路处理动作。包括以下几种：

- Block：阻塞指定接口并发送 Trap 信息。
- Trap-only：只发送 Trap 信息。
- Shutdown：关闭指定接口并发送 Trap 信息。
- Shutdown-restore：发送 trap，关闭端口并等待恢复

环路检测模式

环路检测模式为 Port 模式。

Port 模式：出现环路时，若环路处理方式为 Block，则阻塞接口并发送 Trap；若环路处理方式为 Shutdown 方式，则关闭物理接口并发送 Trap。

若环路处理方式为 Trap-only，则只发送 Trap 信息。

环路恢复

接口由于环路被关闭之后，可以根据用户配置于指定时间后自动恢复。

9.6.2 配置准备

场景

在网络中，所有接入设备下连的主机或二层设备都可能存在有意、无意的连接而引起的环路，在每台接入设备上开启环路检测功能，可以避免网络环路造成数据流无限制复制而形成的网络拥塞状况。

前提

设备上环路检测、接口备份、STP、G.8032 功能之间可能会相互影响，建议不要同一接口上同时开启这些功能。

9.6.3 环路检测的缺省配置

设备上环路检测的缺省配置如下。

功能	缺省值
环路检测功能状态	禁止
接口阻塞后的自动恢复时间	5s

功能	缺省值
环路检测处理方式	block
环路检测报文发送周期	1s
环路检测模式	vlan 模式

9.6.4 配置环路检测功能

请在设备上进行以下配置。

说明

环路检测与生成树协议冲突，二者不能同时开启。

直连设备两端不能同时开启环路检测。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**loopback-detect mode vlan**	配置基于 VLAN 的环路检测功能。
4	JX(config-ge-1/0/*)#**loopback-detect vlan** *vlan-list*	配置发包 vlan
5	JX(config-ge-1/0/*)#**loopback-detect action block**	配置环路动作
6	JX(config)#**loopback-detect interval** *interval*	配置发包间隔，单位：秒
7	JX(config)#**loopback-detect recovery-interval** *interval*	配置恢复时间，单位：秒

9.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show loopback-detect interface**	查看接口环路检测配置。

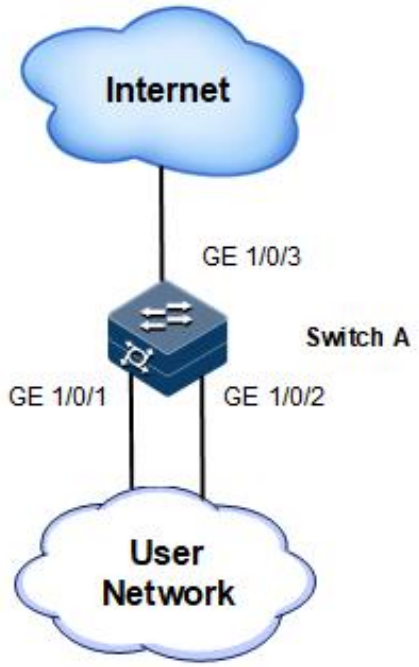
9.6.6 配置环路检测内环应用示例

组网需求

如下图所示，Switch A 通过 GE 1/0/1 和 GE 1/0/2 接口连接 VLAN 3 用户网络，为了避免用户网络中存在环路，需要在 Switch A 上开启环路检测功能，及时检测用户网络中的环路并进行处理。具体要求如下：

- 使能 GE 1/0/1 和 GE 1/0/2 接口的环路检测功能。
- 配置环路检测报文发送间隔为 3s。
- 配置环路检测模 VLAN 为 VLAN3。
- 配置 GE 1/0/2 接口的环路检测处理动作为 Block，发送告警信息并阻塞接口。

图 9-18 环路检测内环应用组网示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 3
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type hybrid
JX(config-ge-1/0/1)#port hybrid vlan 3 untagged
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/1)#port link-type hybrid
```

```
JX(config-ge-1/0/2)#port hybrid vlan 3 untagged
JX(config-ge-1/0/2)#exit
```

步骤 2 配置环路检测 VLAN、环路检测处理动作和环路检测报文发送周期。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#loopback-detect enable
JX(config-ge-1/0/1)#loopback-detect action block
JX(config-ge-1/0/1)#loopback-detect vlan 3
JX(config-ge-1/0/1)#loopback-detect interval 3
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#loopback-detect enable
JX(config-ge-1/0/2)#loopback-detect action block
JX(config-ge-1/0/2)#loopback-detect vlan 3
JX(config-ge-1/0/2)#loopback-detect interval 3
```

检查结果

通过 **show loopback-detect interfac** 命令查看接口环路检测状态，此时没有环路。

```
JX#show loopback-detect interface
 Interface     Enable  Action        Loop-Status
------------------------------------------------------------
 ge-1/0/1      enable  block         none-loop
 ge-1/0/2      enable  block         none-loop
------------------------------------------------------------
```

9.7 端口备份

9.7.1 简介

双上行组网是目前常用的应用组网之一，该组网下常通过生成树协议（STP，Spanning Tree Protocol）阻塞冗余链路，起备份作用。虽然这种方案从功能上可以实现客户冗余备份的需求，但是在性能上却不能达到很多用户的要求，即使采用快速生成树协议的快速迁移，也只能是秒级的收敛速度。这对于应用于电信级网络核心的高端以太网交换机，是非常不利的一个性能参数。

接口备份解决方案针对双上行组网，实现主备链路冗余备份及快速迁移。该方案为双上行组网量身定做，既保证了性能，又简化了配置。

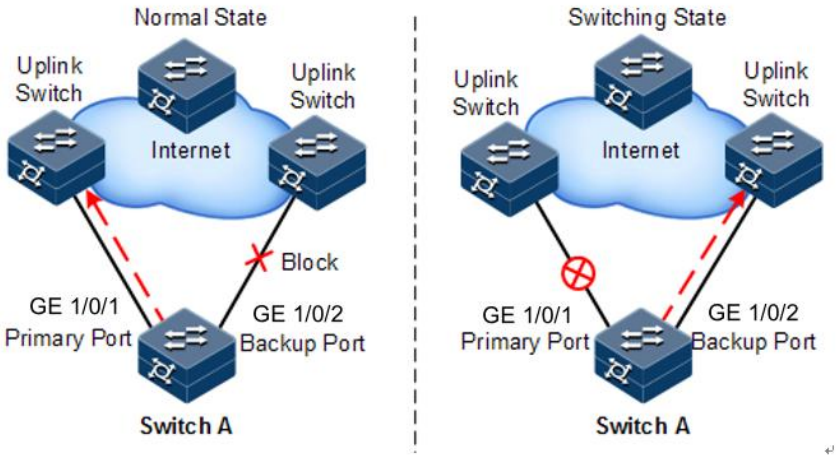
接口备份功能是 STP 协议的另一个解决方案，用户可以在关闭 STP 功能的情况下，通过手动设置接口实现基本的链路冗余。如果交换机已经开启 STP，就需要禁止接口备份功能，因为 STP 已经提供了类似的功能。

端口备份原理

接口备份功能需要设置接口备份组来实现。接口备份组包括一对接口，其中一个接口是主接口，另一个接口是备份接口。主接口所在的链路称为主链路，备份接口所在的链路称为备份链路。接口备份组的成员接口支持物理接口和链路聚合组，不支持三层接口。

在接口备份组中，当一个接口处于转发（Forward）状态时，另一个接口则处于阻塞状态（Block）。任何时刻，两个接口中只有一个接口处于转发状态。当处于转发状态的接口发生链路故障时，处于待命状态的接口才会切换到转发状态，以保持链路正常。

图 9-19 接口备份原理示意图



接口备份原理如上图所示。Switch A 上的 GE 1/0/1、GE 1/0/2 分别与上行交换机相连，接口转发状态如下：

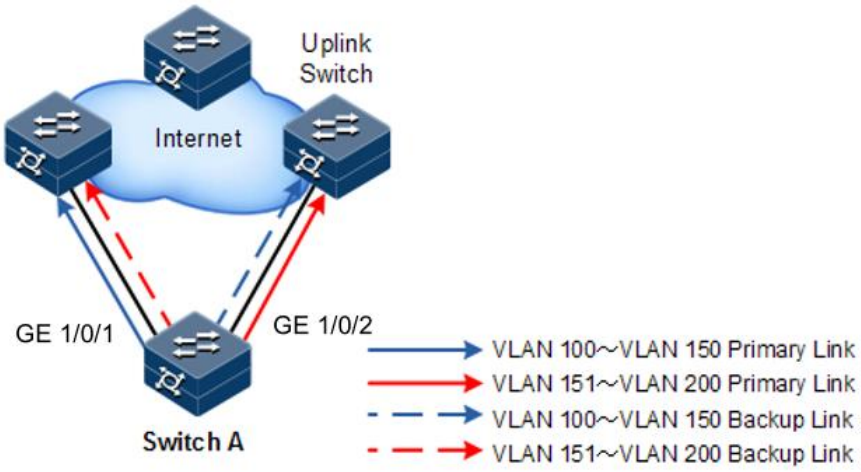
- 正常状态下，Switch A 的 GE 1/0/1 为主接口，GE 1/0/2 为备份接口，GE 1/0/1 和上行交换机之间转发报文，GE 1/0/2 和上行交换机之间不转发报文。
- 当 GE 1/0/1 与上行交换机之间出现链路故障时，备份接口 GE 1/0/2 和上行交换机之间转发报文。
- 当 GE 1/0/1 链路故障恢复并保持一段时间（恢复延时）后，GE 1/0/1 变为转发状态，GE 1/0/2 变为待命状态。

如果主接口和备份接口之间发生切换，交换机会发送一个 Trap 上报网管系统。

接口备份在不同 VLAN 上的应用

接口备份通过在 VLAN 上进行应用，还可以实现两个接口在不同 VLAN 上同时进行转发，如下图所示。

图 9-20 接口备份在不同 VLAN 上的应用原理示意图



在不同的 VLAN 上，接口的转发状态如下：

- 正常情况下，配置 Switch A 在 VLAN 100～VLAN 150 上，Gigaethernet 1/0/1 为主接口，Gigaethernet 1/0/2 为备份接口；在 VLAN 151～VLAN 200 上，Gigaethernet 1/0/2 为主接口，Gigaethernet 1/0/1 为备份接口。那么，Gigaethernet 1/0/1 在 VLAN 100～VLAN 150 转发流量，Gigaethernet 1/0/2 在 VLAN 151～VLAN 200 上转发流量。
- 当 Gigaethernet 1/0/1 发生链路故障时，Gigaethernet 1/0/2 负责转发 VLAN 100～VLAN 200 上的流量。
- 当 Gigaethernet 1/0/1 恢复正常并保持一段时间（恢复延时）后，Gigaethernet 1/0/1 在 VLAN 100～VLAN 150 上转发流量，Gigaethernet 1/0/2 在 VLAN 151～VLAN 200 上转发流量。

利用这种方法，接口备份可以用于负载均衡。同时，这种应用不依赖于上联交换机的配置，便于用户操作。

9.7.2 配置准备

场景

在双上行网络中，通过配置端口备份功能，可以实现主备链路的冗余备份及其快速倒换。通过在不同 VLAN 中应用端口备份，还可以实现各端口之间的负载分担。

与 STP 功能相比，端口备份功能既保证了毫秒级的倒换性能，又简化了配置。

前提

无

9.7.3 接口备份的缺省配置

设备上接口备份的缺省配置如下。

功能	缺省值
接口备份组	无
故障恢复延时时间	15s
恢复模式	不返回模式

9.7.4 配置接口备份基本功能

注意

设备上接口备份与 STP、环路检测和 ERPS 功能之间可能会相互影响，建议不要在同一接口上同时开启这些功能。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**protect-link group** *group-id*	创建备份组
3	JX(config-protectlink-*)#**protect-vlan** *vlan-list*	配置指定的 VLAN 列表
4	JX(config-protectlink-*)#**add interface** *interface-type interface-number* **role master**	指定主接口
5	JX(config-protectlink-*)#**add interface** *interface-type interface-number* **role slave**	指定备份接口
6	JX(config-protectlink-*)#**reverse { enable | disable }**	配置恢复模式。
7	JX(config-protectlink-*)#**reverse time** *interval*	配置恢复时间

说明

- 在一个接口备份组中，一个接口不能既是主接口，又是备份接口。
- 在同一 VLAN 上，一个接口/链路聚合组不能同时充当两个接口备份组的成员。

9.7.5 配置接口强制倒换

注意

- 配置强制倒换成功后，主备链路将进行倒换，工作链路被强制倒换到备份链路上。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**protect-link group** *group-id*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-protectlink-*)#**manual-switch**	配置接口强制倒换。

9.7.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show protect-link interface**	查看接口备份相关的状态信息。
2	JX#**show protect-link group**	查看接口备份组相关的配置信息。

9.7.7 配置接口备份示例

组网需求

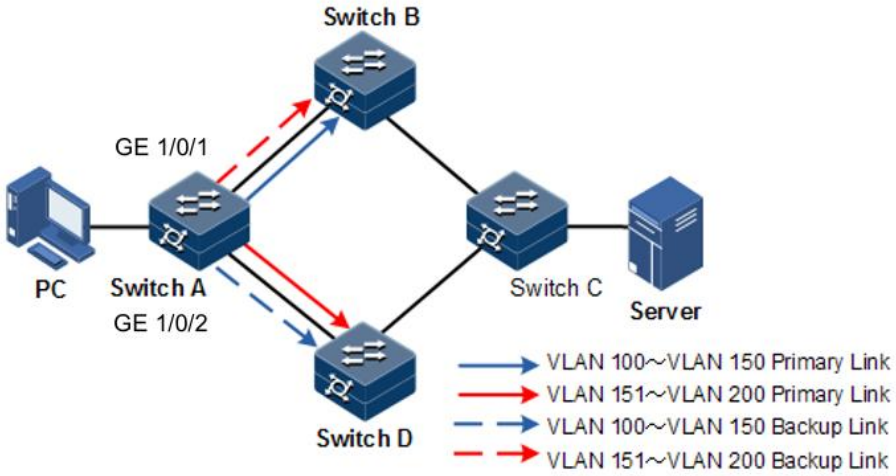
如下图所示，为实现远程 PC 到服务器的可靠访问，需要在 Switch A 上配置接口备份组，并指定 VLAN 列表，实现接口链路保护和负载分担。其要求如下：

- 配置 Switch A 在 VLAN 100～VLAN 150 上，GE 1/0/1 为主接口，GE 1/0/2 为备份接口；
- 配置 Switch A 在 VLAN 151～VLAN 200 上，GE 1/0/2 为主接口，GE 1/0/1 为备份接口。

当 GE 1/0/1 发生链路故障时，切换到备份接口 GE 1/0/2，以保持链路正常。

Switch A 需要支持接口备份功能，Switch B、Switch C、Switch D 无需支持接口备份功能。

图 9-21 接口备份应用组网示意图



配置步骤

步骤 1 创建 VLAN 100～VLAN 200，并将 GE 1/0/1 和 GE 1/0/2 加入到 VLAN 100～VLAN 200 中。

```
JX#configure
JX(config)#vlan 100-200
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 100-200
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type trunk
JX(config-ge-1/0/2)#port trunk allow-pass vlan 100-200
JX(config-ge-1/0/2)#exit
```

步骤 2 在 VLAN 100～VLAN 150 上配置 GE 1/0/1 为主接口，GE 1/0/2 为备份接口。

```
JX(config)#protect-link group 1
JX(config-protectlink-1)#protect-vlan 100-150
JX(config-protectlink-1)#add interface ge 1/0/1 role master
JX(config-protectlink-1)#add interface ge 1/0/2 role slave
```

步骤 3 在 VLAN 151～VLAN 200 上配置 GE 1/0/2 为主接口，GE 1/0/1 为备份接口。

```
JX(config)#protect-link group 2
JX(config-protectlink-1)#protect-vlan 151-200
JX(config-protectlink-1)#add interface ge 1/0/2 role master
```

```
JX(config-protectlink-1)#add interface ge 1/0/1 role slave
```

检查结果

通过 **show protect-link interface** 命令，分别在正常状态和链路故障情况下查看接口备份相关的状态信息。

当 GE 1/0/1 和 GE 1/0/2 链路均为 Forward 时，GE 1/0/1 在 VLAN 100～VLAN 150 上转发流量，GE 1/0/2 在 VLAN 151～VLAN 200 上转发流量。

```
JX#show protect-link interface
 Interface         Group  Role    State     Status    Linkstate
-------------------------------------------------------------------------
-------
 ge-1/0/1          1      master  forward   active    up/up
 ge-1/0/2          1      slave   block     active    up/up
 ge-1/0/1          2      slave   block     active    up/up
 ge-1/0/2          2      master  forward   active    up/up
-------------------------------------------------------------------------
-------
```

手动断开 Switch A 和 Switch B 之间的链路来模拟故障，此时 GE 1/0/1 变为 Down，则 GE 1/0/2 负责转发 VLAN 100～VLAN 200 上的流量。

```
JX#show protect-link interface
  Interface         Group  Role    State     Status    Linkstate
-------------------------------------------------------------------------
-------
 ge-1/0/1          1      master  block     active    up/down
 ge-1/0/2          1      slave   forward   active    up/up
 ge-1/0/1          2      slave   block     active    up/down
 ge-1/0/2          2      master  forward   active    up/up
-------------------------------------------------------------------------
-------
```

9.8 端口隔离

9.8.1 简介

通过接口隔离特性，用户可以将需要进行控制的接口使能隔离特性，实现接口之间二层数据的隔离，达到类似于接口之间物理隔离效果，既增强了网络的安全性，也为用户提供了灵活的组网方案。

配置接口保护后，在使能接口保护的接口之间报文不能互通，使能接口保护的接口和未使能接口保护的接口之间的通信不会受影响。

9.8.2 配置准备

场景

通过配置接口隔离功能，可以实现接口之间互相隔离，能增强网络的安全性，也为用户提供了灵活的组网方案。

前提

无

9.8.3 接口隔离的缺省配置

设备上接口隔离的缺省配置如下。

功能	缺省值
各接口的接口隔离功能状态	禁止

9.8.4 配置接口隔离

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**port-isolate group** *group-id*	创建隔离组。
3	JX(config-isolate-group-1)#**add interface** *interface-type interface-number*	将接口加入隔离组

9.8.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

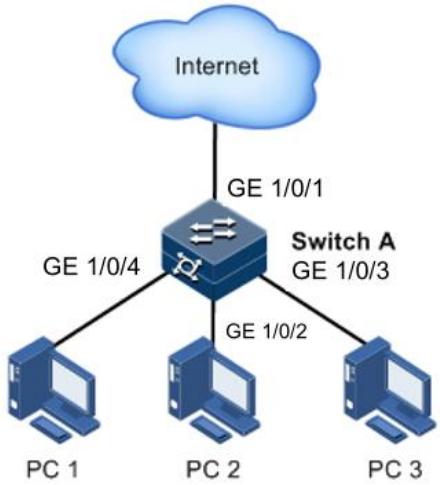
序号	检查项	说明
1	JX#**show port-isolate information**	查看接口保护配置。
2	JX#**show port-isolate group**	查看接口隔离配置信息。

9.8.6 配置接口保护示例

组网需求

如下图所示，为了使 PC1 和 PC2 之间不能互通，但 PC 1 和 PC 2 可以分别与 PC 3 通信，可以在 Switch A 的 GE 1/0/4 和 GE 1/0/2 接口上开启接口保护功能。

图 9-22 接口保护组网示意图



配置步骤

步骤 1 创建端口隔离组。

```
JX#configure
JX(config)#port-isolate group 1
```

步骤 2 将 GE 1/0/1 和 GE 1/0/2 加入隔离组。

```
JX(config-isolate-group-1)##add interface ge 1/0/4
JX(config-isolate-group-1)##add interface ge 1/0/2
```

检查结果

通过 **show port-isolate group** 查看接口保护配置是否正确。

```
JX#show port-isolate group
  GroupId       Ports
-------------------------------------------------------------------------------
-------
  1           ge-1/0/2 ge-1/0/4
-------------------------------------------------------------------------------
-------
```

通过 PC 1 ping PC 3、PC 2 ping PC 3 是否能够 ping 通。

- PC 1 ping PC 3，可以 ping 通。
- PC 2 ping PC 3，可以 ping 通。

通过 PC 1 ping PC 2 是否能够 ping 通，查看接口保护功能是否正确。

PC 1 ping PC 2，不能 ping 通，接口保护功能生效。

9.9 L2CP

9.9.1 简介

MEF（Metro Ethernet Forum，城域以太网论坛）引入了服务的概念，如 EPL、EVPL、EP-LAN 和 EVP-LAN 等六种服务类型，每种服务对 L2CP（Layer 2 Control Protocol，二层控制协议）报文的处理方式不同。

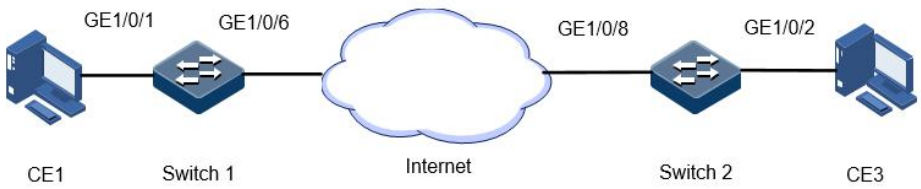
在 MEF6.1 中定义了 L2CP 报文的处理方式，分别为：

- discard：丢弃报文。
- peer：上交到 cpu。
- tunnel：传递到城域网，处理方式配置相比 discard 和 peer 较为复杂。需通过将用户网络侧接口的匹配规则和运营商侧接口 tunnel 终端的配合使用，才能使报文穿过运营商网络。

9.9.2 配置准备

场景

图 9-23 L2CP 拓扑图



switch1,switch2 交换机作为运营商网络接入设备，CE1，CE3 作为用户网络接入设备，CE1，CE3 分别与 switch1 的 ge 1/0/1,switch2 的 ge 1/0/2 相连。

通过配置不同用户网络的 L2PROTOCOL 报文透明传输，使得：

用户网络中的设备可以共同完成生成树功能

前提

无

9.9.3 缺省配置

功能	缺省值
L2CP 功能	未使能

9.9.4 配置 L2CP

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface interface-type** *interface-number*	进入接口配置模式。
3	JX(config-ge-1/0/1)#**l2cp { uni | nni | disable }**	使能 l2cp 功能 uni：用户侧接口 nni：网络侧接口 disable：去使能端口角色 缺省为没有角色
4	JX(config-ge-1/0/1)#**l2cp known-protocol {cdp|eoam3ah|gmrp |gvrp|hgmp|lacp|lldp|pagp|stp |udld|vtp|lamp|esmc |dot1x |elmi|pvst} [vlan** *vlan-id* **] action tunnel group-mac** *mac-address*	在 uni 接口上配置替换规则 known-protocol：匹配的协议名称 mac-address：替换的组播 mac 地址 vlan-id：匹配 vlan id
5	JX(config-ge-1/0/1)#**l2cp protocol-mac** *dst-mac-address* **[vlan** *vlan-id* **] action tunnel group-mac** *mac-address*	在 uni 接口上配置替换规则 dst-mac-address：匹配的目的 mac 地址 mac-address：替换的组播 mac 地址 vlan-id：匹配 vlan id

步骤	配置	说明
6	JX(config-ge-1/0/1)#**l2cp known-protocol {cdp|eoam3ah|gmrp |gvrp|hgmp|lacp|lldp|pagp|stp |udld|vtp|lamp|esmc |dot1x |elmi|pvst} action { peer | discard }**	在 uni 接口上配置上送或丢弃规则 known-protocol：匹配的协议名称 peer：上送 CPU discard：丢弃
7	JX(config-ge-1/0/1)#**l2cp protocol-mac** *dst-mac-address* **action { peer | discard }**	在 uni 接口上配置上送或丢弃规则 dst-mac-address：匹配的目的 mac 地址 peer：上送 CPU discard：丢弃

9.9.5 检查配置

步骤	配置	说明
1	JX#**show l2cp**	显示 l2cp 全局信息。
2	JX#**show l2cp config**	显示 l2cp 配置信息。
3	JX#**show protocol statistics rx with-value**	显示 l2cp 上送 CPU 的报文统计

9.9.6 配置 L2CP 示例

配置步骤

步骤 1 配置 CE-1：

```
JX(config)#stp enable
```

步骤 2 配置 CE-3：

```
JX(config)#stp enable
```

步骤 3 配置 switch1：

```
JX(config-ge-1/0/1)#l2cp uni
JX(config-ge-1/0/1)#l2cp known-protocol stp action tunnel group-mac
01:00:0c:cd:cd:d0
JX(config-ge-1/0/6)#l2cp nni
```

步骤 4 配置 switch2：

```
JX(config-ge-1/0/2)#l2cp uni
JX(config-ge-1/0/2)#l2cp known-protocol stp action tunnel group-mac
01:00:0c:cd:cd:d0
JX(config-ge-1/0/8)#l2cp nni
```

检查配置

CE1 和 CE3 上分别可以看到对方的生成树信息

9.10 BFD

9.10.1 简介

双向转发检测 BFD（Bidirectional Forwarding Detection）是一种全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况。

9.10.2 配置准备

场景

BFD 在两台网络设备上建立会话，用来检测网络设备间的双向转发路径，为上层应用服务。BFD 本身并没有邻居发现机制，而是靠被服务的上层应用通知其邻居信息以建立会话。会话建立后会周期性地快速发送 BFD 报文，如果在检测时间内没有收到 BFD 报文则认为该双向转发路径发生了故障，通知被服务的上层应用进行相应的处理。

前提

无

9.10.3 BFD 的缺省配置

设备上接口隔离的缺省配置如下。

功能	缺省值
全局 BFD 功能	未使能
发送间隔	1000 毫秒
接收间隔	1000 毫秒
本地检测倍数	3

9.10.4 配置 BFD 单臂回声会话

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**bfd start**	全局使能 bfd。
3	JX(config)#bfd track 1 remote-ip 10.0.0.2 local-ip 10.0.0.1 interface vlan 1 one-arm-echo	配置单臂 ECHO 功能的 BFD 会话。
4	JX(config)#bfd track 1 remote-ip6 2001::2 local-ip6 2001::1 interface vlan 1 one-arm-echo	配置单臂 ECHO 功能的 BFD 会话。

9.10.5 配置 BFD 会话参数

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**bfd start**	全局使能 bfd。
3	JX(config)#**bfd track** *track-number* **remote-ip** *remote-ip-address* **local-ip** *local-ip-address*	创建会话。
4	JX(config)#**bfd track** track-number **min-tx** { value | **default** } [**local-discriminator** *local-value* [**min-rx** { *value* | **default** } [**multiplier** { *local-value* | **default** } [**remote-dicriminator** { *remote-value* | **default** }]]]] JX(config)#**bfd track** track-number **min-rx** { value | **default** } [**local-discriminator** *local-value* [**min-tx** { *value* | **default** } [**multiplier** { *local-value* | **default** } [**remote-dicriminator** { *remote-value* | **default** }]]]]	配置会话参数。

9.10.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

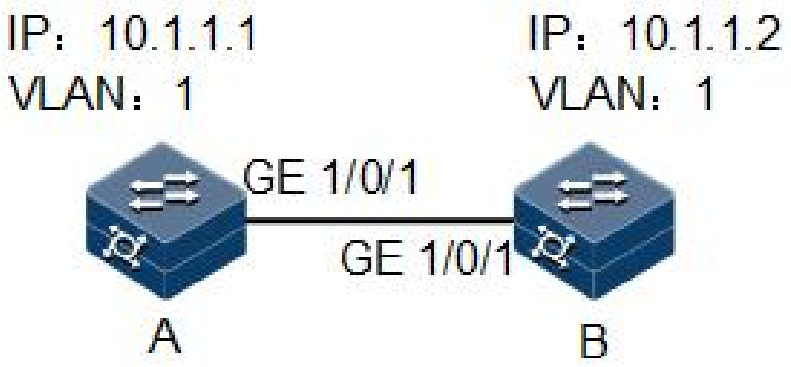
序号	检查项	说明
1	JX#**show bfd session**	查看 bfd 会话。
2	JX#**show bfd track**	查看 bfd track。

9.10.7 配置 BFD 单跳应用示例

组网需求

如下图所示，配置 B • FD 单跳会话检测设备 A、B 之间的链路状态。

图 9-24 BFD 单跳应用



配置步骤

步骤 1 配置 A 设备 IP 和会话参数。

```
JX#configure
JX(config)#interface vlan 1
JX(config)#ip address 10.1.1.1/24
JX(config)#bfd track 1 remote-ip 10.1.1.2 local-ip 10.1.1.1
JX(config)#bfd track 1 min-tx 500 min-rx 600 multiplier 3
```

步骤 2 配 A 设备 IP 和会话参数。

```
JX#configure
JX(config)#interface vlan 1
JX(config)#ip address 10.1.1.1/24
JX(config)#bfd track 1 remote-ip 10.1.1.1 local-ip 10.1.1.2
JX(config)#bfd track 1 min-tx 500 min-rx 600 multiplier 4
```

检查结果

通过 **show bfd session** 查看会话状态

```
JX#show bfd session
  Interface      State Local-Discr Remote-Discr local-addr       remote-
addr
------------------------------------------------------------------------
------------------
  vlan-1         up    1           1           10.1.1.1         10.1.1.2
```

9.11 链路震荡保护

9.11.1 简介

链路震荡保护（Link-flap Protection）是一种将物理状态频繁 Up/Down 变化的接口关闭，使之处于 Down 状态，防止网络拓扑结构频繁变化的技术。

9.11.2 配置准备

场景

网络抖动或者链路线路故障等原因会引起本端设备接口物理状态频繁 Up/Down 变化，导致链路震荡，致使网络拓扑结构频繁变化，影响用户通信。为了解决上述问题，用户可以配置链路震荡保护，将物理状态频繁 Up/Down 的接口关闭，使之处于 Down 状态，使网络拓扑结构停止频繁变化。

链路震荡次数：接口状态 Up/Down 切换一次，记为一次震荡。

链路震荡检测时间间隔：系统需要统计指定时间间隔内链路震荡的次数。

如果在链路震荡检测时间间隔内，链路震荡次数达到了门限值，则将该端口关闭。

前提

无

9.11.3 链路震荡保护的缺省配置

设备上接口链路震荡保护的缺省配置如下。

功能	缺省值
使能链路震荡保护	未使能
链路检测检测时间间隔	10 秒
链路震荡次数	5 次

9.11.4 配置链路震荡保护

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/*)#**port link-flap protection** { **enable** | **disable** }	配置链路震荡保护使能或去使能。
4	JX(config)#**port link-flap interval** { *60* | **default**}	配置链路震荡检测时间间隔。
5	JX(config)#**port link-flap threshold** { *7* | **default**}	配置链路震荡次数门限值。

9.11.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show link-flap config**	查看链路震荡保护相关配置。
2	JX#**show link-flap interface**	查看链路震荡保护相关接口信息。

9.11.6 配置链路震荡保护应用示例

配置步骤

步骤 1 配置 A 设备链路震荡保护相关参数。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-flap protection enable
JX(config-ge-1/0/1)#port link-flap interval 60
JX(config-ge-1/0/1)#port link-flap threshold 7
```

检查结果

通过 show link-flap interface 查看链路震荡保护接口状态

```
JX#show link-flap interface
 Error-down recovery interval   : 0
 Interface         Status     Interval    Threshold
-------------------------------------------------------------------------
 ge-1/0/1          enable     60          7
-------------------------------------------------------------------------
```

9.12 接口环回

9.12.1 简介

当网络出现故障或者设备提供服务之前，可以通过在设备上配置接口环回相关命令，检测设备与其他设备之间网络的连通性以及网络质量。

9.12.2 配置准备

场景

设备提供服务之前，为了保证链路的连通性，可以在设备上配置接口环回功能相关命令，从测试设备发送测试报文达到设备的测试端口，设备将测试报文中的源 MAC 和目的 MAC 进行交换，从端口环回到测试设备，进而获取设备与测试设备之间网络的连通性和网络质量信息。

前提

无

9.12.3 接口环回的缺省配置

设备上接口环回的缺省配置如下。

功能	缺省值
接口环回	未使能
接口环回时长	无

9.12.4 配置接口环回

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/*)#**loopback-mode** {**none** | **remote**} [**interval** *interval*]	配置接口环回模式以及测试时长。

9.12.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show interface loop-status**	查看接口环回相关配置以及状态。

9.12.6 配置接口环回应用示例

配置步骤

步骤 1 配置接口环回。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#loopback-mode remote
```

检查结果

通过 **show interface loop-status** 查看接口环回相关信息。

```
JX(config-ge-1/0/1)#show interface loop-status
  Interface             Mode          HoldTime(min)
-------------------------------------------------------------
  ge-1/0/1              remote         forever
  ge-1/0/2              none          forever
  ge-1/0/3              none          forever
  ge-1/0/4              none          forever
  ge-1/0/5              none          forever
  ge-1/0/6              none          forever
  ge-1/0/7              none          forever
  ge-1/0/8              none          forever
  ge-1/0/9              none          forever
  ge-1/0/10             none          forever
  ge-1/0/11             none          forever
  ge-1/0/12             none          forever
-------------------------------------------------------------
```

10 系统管理

本章介绍系统管理与维护特性的基本原理和配置过程，并提供相关的配置案例。

- SNMP
- RMON
- LLDP
- 端口镜像
- 电缆诊断
- UDLD
- 光模块数字诊断
- 系统日志
- 告警管理
- CPU 监控
- 内存监控
- Ping
- Trace
- 硬件监控
- 风扇监控
- 设备堆叠
- MAD
- NQA
- POE
- U 盘部署
- PATCH 补丁功能
- 定时备份配置功能

10.1 SNMP

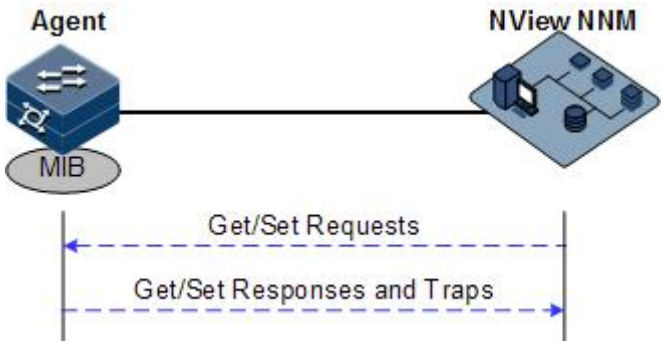
10.1.1 简介

SNMP（Simple Network Management Protocol，简单网络管理协议）是由 IETF（Internet Engineering Task Force，互联网工程任务组）为了解决 Internet 中网络设备的管理问题而提出的一套网络管理协议。SNMP 可以使一个网管系统远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件告警等。它是目前 TCP/IP 网络中应用最广泛的网络管理协议。

工作机制

SNMP 的结构分为代理 Agent 和网管系统两部分。代理和网管系统之间是通过 UDP 传送 SNMP 报文进行通信。SNMP 工作机制如图 10-1。

图 10-1 SNMP 工作机制示意图



甲信 NView NNM 网管系统能够提供友好的人机交互界面，方便网络管理员完成网络管理工作，主要可以实现以下功能：

- 向被管设备发送请求报文。
- 接收来自被管设备的响应报文和 Trap 报文，并显示结果。

代理是驻留在被管设备上的一个进程，主要实现以下功能：

- 接收、响应来自 NView NNM 网管系统的请求报文。
- 根据报文类型，对其进行读或写操作，并生成响应报文，返回给 NView NNM 网管系统。
- 根据各协议模块对触发条件进行定义，在达到触发条件后进入系统、退出系统、设备重新启动等，响应的模块通过代理向 NView NNM 网管系统发送 Trap 报文，报告设备的当前状态。

说明

代理可以同时配置多个版本，采用不同的版本与不同的网管系统交互。但是当代理和某个网管系统通信时，代理和该网管系统上的 SNMP 版本配置必须相同，才能正确互通。

协议版本

目前，SNMP 协议共有 v1、v2c 和 v3 三个版本。

- SNMPv1 采用共同体名（Community Name）认证机制。共同体名用来定义 SNMP 网管系统和 SNMP 代理之间的关系，起到了类似于密码的作用，用来限制 SNMP 网管系统对 SNMP 代理的访问。如果 SNMP 报文携带的共同体名在设备上没有认证通过，该报文将被丢弃。
- SNMPv2c 也采用共同体名认证机制。它在兼容 SNMP v1 的同时又扩充了 SNMP v1 的功能：支持更多的操作类型、数据类型和错误代码、能够更细致地区分错误。
- SNMPv3 采用了 USM（User-Based Security Model，基于用户的安全模型）和 VACM（View-based Access Control Model，基于视图的访问控制模型）安全机制。用户可以设置认证和加密功能，通过有无认证和有无加密等功能组合，可以为 SNMP 网管系统和 SNMP 代理之间的通信提供更高的安全性。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对网管系统和代理之间的传输报文进行加密，以免被窃听。

设备同时支持 SNMP 的 v1、v2c、v3 三个版本。

MIB

MIB（Management Information Base，管理信息库）是网管系统能够管理的所有的对象的集合。它定义了被管理对象的一些属性：

- 名字
- 访问权限
- 数据类型

通过对这些数据项目的存取访问，就可以得到与设备相关的统计内容。每个代理都有自己的 MIB。MIB 可以看成是网管系统和代理之间的一个接口，通过这个接口，网管系统可以对代理中的每一个被管对象进行读/写操作，从而达到管理和监控设备的目的。

MIB 采用树形结构进行存储，它的根在最上面，没有名字。树的节点表示被管理对象，它可以从根开始的一条路径唯一地识别（OID）。SNMP 协议报文通过遍历 MIB 树形目录中的节点来访问网络中的设备。

设备支持标准的 MIB 库和甲信自定义的 MIB 库。

10.1.2 配置准备

场景

当用户需要通过网管系统登录交换机设备时，应首先对设备配置 SNMP 基本功能。

前提

在配置 SNMP 之前，需完成以下任务：

- 配置路由协议，使设备和网管系统之间路由可达。

10.1.3 SNMP 的缺省配置

设备上 SNMP 的缺省配置如下。

功能	缺省值
SNMP 服务	缺省关闭，需要手动配置开启
SNMP 视图	缺省存在：internet 视图
SNMP 共同体	缺省存在：public、private 共同体
SNMP 访问组	缺省不存在
SNMP 用户	缺省不存在
SNMP 用户和访问组的映射关系	无
网管人员的标识和联系方法	support@JX.com
设备放置的物理位置	World China JX
Trap 状态	使能
SNMP 目标主机地址	无
SNMP 引擎 ID	800022B603000000111233

10.1.4 配置 SNMP v1/v2c 基本功能

SNMP Agent 为了保护自身及其管理的 MIB 不被非法访问，提出了共同体的概念。在某一个共同体内的管理站必须在所有对 Agent 的操作中使用该共同体的名字，否则其请求不被受理。

共同体名是用不同的字符串来标识不同的 SNMP 团体。不同的共同体可以具有只读（read-only）或读写（read-write）访问权限。具有只读权限的团体只能对设备信息进行查询，具有读写权限的团体除了可以对设备信息进行查询之外还可以对设备进行配置。

SNMP v1/v2c 采用共同体名认证方案，与设备认可的共同体名不符合的 SNMP 报文将被丢弃。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**snmp server start**	启动 SNMP 服务端功能。

步骤	配置	说明
3	JX(config)#**snmp mib-view** *view-name* { **included** | **excluded** } *oid-tree* [**mask** *subtree-mask*]	创建 SNMP 视图，并配置访问的 MIB 变量范围。 缺省视图是 internet，范围包括 MIB 树中“1.3.6”节点以下的所有 MIB 变量。
4	JX(config)#**snmp community** { **read** | **write** } { **cipher** | **plain** } *community-name* [**mib-view** *view-name* |**acl-ipv4** *acl-ipv4-number* |**acl-ipv6** acl-ipv6-number]*	创建共同体名并配置对应的视图和访问权限。 如果没有填写 **mib-view** *view-name* 选项，则采用缺省视图 internet。

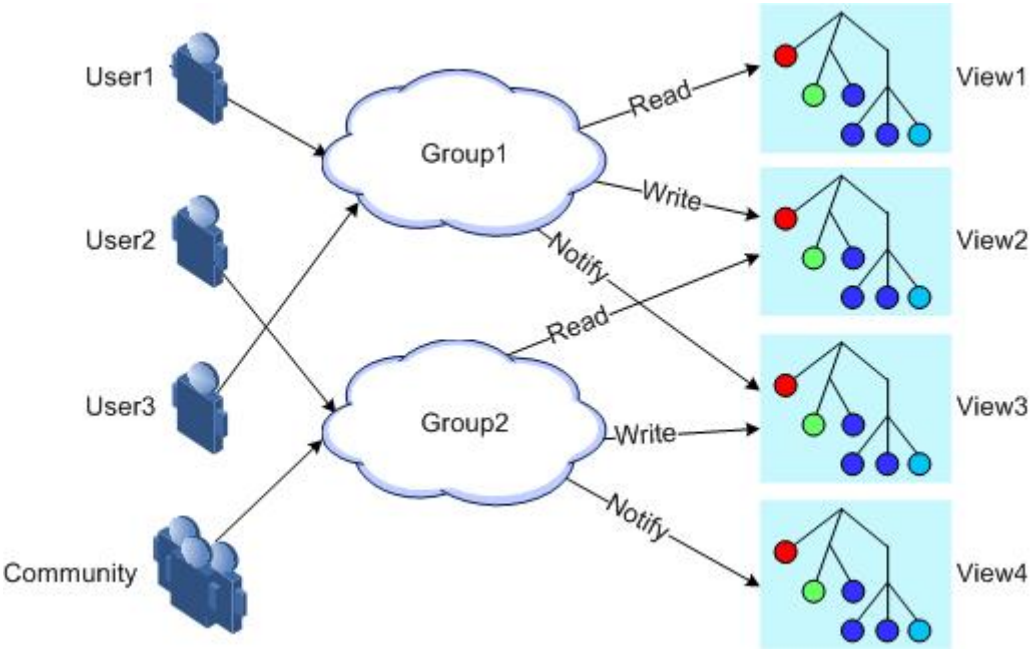
10.1.5 配置 SNMP v3 基本功能

SNMPV3 采用 USM 基于用户的认证机制。USM 提出了访问组（Group）的概念：一个或多个用户对应于一个访问组，每个访问组设定相应的读、写、通告视图，访问组中的用户拥有在该视图内的权限。发送 Get 和 Set 等请求的用户所在的访问组必须具有和其请求相应的权限，否则请求不被受理。

如图 10-2 所示，网管站采用 SNMP v3 对交换机正常的访问，需要进行的配置如下：

- 配置用户
- 确定用户属于哪个访问组
- 配置访问组拥有的视图权限
- 创建视图

图 10-2 SNMP v3 认证机制示意图



请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**snmp mib-view** *view-name* { **included** | **excluded** } *oid-tree* [**mask** *subtree-mask*]	创建 SNMP 视图，并配置访问的 MIB 变量范围。 缺省视图是 internet，范围包括 MIB 树中“1.3.6”节点以下的所有 MIB 变量。
3	JX(config)#**snmp group** *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view-name* | **write-view** *write-view-name* | **notify-view** *notify-view-name*]*	配置访问组相关。
4	JX(config)#**snmp user** *user-name* **group** *group-name* **authentication** { **md5** | **sha** } *authpassword* **privacy** { **des** | **aes** } *privkeypassword*	创建用户并绑定组，并配置认证和加密。
5	JX(config)#**snmp user** *user-name* **group** *group-name* **authentication** { **md5** | **sha** } *authpassword*	创建用户并绑定组，并配置认证方式。
6	JX(config)#**snmp user** *user-name* **group** *group-name* [**acl-ipv4** *acl-ipv4-number* | **acl-ipv6** *acl-ipv6-number*]*	创建用户并绑定访问组。

10.1.6 配置 SNMP 其他信息

SNMP v1、v2c、v3 均支持以下信息的配置。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**snmp contact** *string*	配置联系方法。
3	JX(config)#**snmp location** *location-string*	配置设备当前所在地址信息。
4	JX(config)#**snmp auth-fail-reply** { **enable** | **disable** }	配置在认证失败时是否发送 SNMP 响应报文。
5	JX(config)#**snmp auth-trap** { **enable** | **disable** }	配置是否使能认证 Trap。

步骤	配置	说明
6	JX(config)#**snmp auth-fail-count** *fail-count-value*	配置 SNMP 认证失败次数。
7	JX(config)#**snmp reauth-interval** *reauth-interval-value*	配置 SNMP 重认证时间。
8	JX(config)#**snmp packet max-size** { *size-value*|**default** }	配置 SNMP 收发包最大长度。
9	JX(config)#**snmp reply-source-ip** { **enable** | **disable** }	配置将所输入的 IP 地址作为应答报文的源地址
10	JX(config)#**snmp udp-port** { *port-number* | **default** }	配置 SNMP 服务端口号。

10.1.7 配置 Trap

说明

SNMP v1、v2c 和 v3 的 Trap 配置步骤除了目标主机的配置，其余都是一样的，请根据需要进行选择。

支持同时向多个 Trap 目标主机发送 Trap 告警信息，在设备上配置多个 Trap host 即可。

Trap 是设备主动向网管系统发送的未经请求的信息，用于报告一些紧急的重要事件。

在配置 Trap 功能之前，需完成以下任务：

- 配置 SNMP 的基本功能。如果使用 SNMP v1 和 v2c 版本需要配置共同体名；如果使用 SNMP v3 版本需要配置用户名和 SNMP 视图。
- 配置路由协议，使设备和网管系统之间路由可达。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**snmp server** { **start** | **stop** }	启动 SNMP 服务端功能。
3	JX(config)#**snmp trap-host** *ip-address* { **v1** | **v2** } [**port** *port-id* | **securityname** *security-name*]*	配置基于 SNMP v1 和 SNMP v2c 的 Trap 目标主机(IPV4)。
4	JX(config)#**snmp-ipv6 trap-host** *ipv6-address* { **v1** | **v2** } [**port** *port-id* | **securityname** *security-name*]*	配置基于 SNMP v1 和 SNMP v2c 的 Trap 目标主机(IPV6)。

步骤	配置	说明
5	JX(config)#**snmp trap-host** *ip-address* **v3** { **authentication** | **privacy** } **securityname** *security-name* [**port** *port-id*]	配置基于 SNMP v3 的 Trap 目标主机(IPV4)。
6	JX(config)#**snmp-ipv6 trap-host** *ipv6-address* **v3** { **authentication** | **privacy** } **securityname** *security-name* [**port** *port-id*]	配置基于 SNMP v3 的 Trap 目标主机 IPV6)。

10.1.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

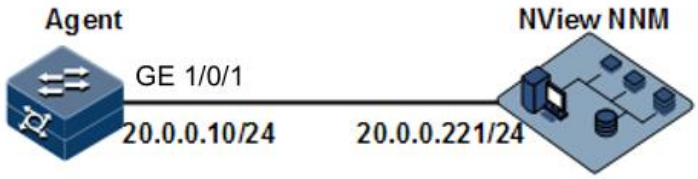
序号	检查项	说明
1	JX#**show snmp information**	查看 SNMP 全局的信息。 包含本地 SNMP 引擎 ID，网管人员的标识及联系方法，设备所在位置，Trap 开关状态信息，SNMP 服务开启状态，服务端口号。
2	JX#**show snmp group**	查看 SNMP 访问组的信息。
3	JX#**show snmp community**	查看 SNMP 共同体的配置信息。
4	JX#**show snmp config**	查看 SNMP 的基本配置信息。
5	JX#**show snmp trap-host**	查看 Trap 目标主机信息。
6	JX#**show snmp statistics**	查看 SNMP 的统计信息。
7	JX#**show snmp user**	查看 SNMP 用户信息。
8	JX#**show snmp mib-view**	查看 SNMP 的视图信息。

10.1.9 配置 SNMP v1/v2c 和 Trap 示例

组网需求

如图 10-3 所示，NView NNM 网管系统与交换机设备之间路由可达，NView NNM 通过 SNMP v1/v2c 可以查看远程交换机的对应视图下的 MIB，交换机出现紧急情况时可以主动向 NView NNM 发送 Trap。

图 10-3 SNMP v1/v2c 组网示意图



配置步骤

步骤 1 配置交换机设备的 IP 地址。

```
JX#configure
JX(config)#interface meth 0/0/0
JX(config-meth-0/0/0)#ip address 192.168.62.100/24
JX(config-meth-0/0/0)#quit
```

步骤 2 启动 SNMP 服务端功能。

```
JX(config)#snmp server start
```

步骤 3 配置 Trap 告警。

```
JX(config)#snmp trap-host 192.168.62.1 v2
```

检查结果

通过 **show ip interface** 查看 IP 地址配置是否正确。

```
JX#show ip interface
Total number: 2
 Interface         State(a/o) Addr/Prefix       Role     Type      Vpn-
instance
------------------------------------------------------------------------------
---------------------------
 loopback-0        up/up     127.0.0.1/8       primary  auto      N/A
 meth-0/0/0        up/up     192.168.62.100/24 primary  static    N/A
------------------------------------------------------------------------------
---------------------------
```

通过 **show snmp config** 查看 SNMP 配置是否正确。

```
JX#show snmp config
Software Version: SNMP_VL3.00.00.00
!
snmp server start
snmp trap-host 192.168.62.1 securityname
AJ35Grrnpx3xRv_UdbJBiGsl3Dwxp932il5pfsKvs8X-GN6R49ihEydRaxBXkM5V-w
```

通过 **show snmp trap-host** 查看目标主机配置是否正确。

```
JX#show snmp trap-host
Trap-host : 192.168.62.1
```

```
------------------------------------------------------------------------
-------
Status             : ACTIVE
Udp Port           : 162
MP Modle           : V2
Security Level      : None
Security Name       : AJ35Grrnpx3xRv_UdbJBiGsl3Dwxp932il5pfsKvs8X-
GN6R49ihEydRaxBXkM5V-w
Vpn Instance Name    : public
------------------------------------------------------------------------
-------
```

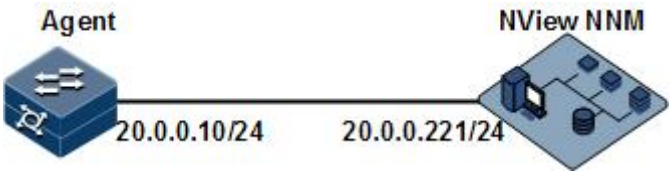
10.1.10 配置 SNMP v3 和 Trap 示例

组网需求

如图 10-4 所示，NView NNM 网管系统与 Agent 之间有可达路由，NView NNM 通过 SNMP v3 对 Agent 进行监控，Agent 出现紧急情况时可以主动向 NView NNM 发送 Trap。

缺省情况下，交换机设备上存在 VLAN 1，所有物理接口属于 VLAN 1。

图 10-4 SNMP v3 和 Trap 组网示意图



配置步骤

步骤 1 配置交换机设备的 IP 地址。

```
JX#configure
JX(config)#interface meth 0/0/0
JX(config-meth-0/0/0)#ip address 192.168.62.100/24
JX(config-meth-0/0/0)#quit
```

步骤 2 配置 SNMP v3 访问。

启动 SNMP 服务端功能。

```
JX(config)#snmp server start
```

创建 g1 的访问组，安全等级为认证但不加密。

```
JX(config)#snmp group g1 authentication
```

创建用户 u1 为认证但不加密，绑定访问组 g1，采用 md5 鉴别算法，口令为 JX。

```
JX(config)#snmp user u1 group g1 authentication md5 JX
```

步骤 3 配置 Trap 告警，配置的 trap-host 类型必须与 user 的认证类型一致，不存在包含关系。

```
JX(config)#snmp trap-host 192.168.62.1 v3 authentication securityname u1
```

检查结果

通过 **show snmp group** 查看 SNMP 访问组信息配置是否正确。

```
JX#show snmp group
Group                          Security     ReadView
WriteView                       NotifyView
------------------------------------------------------------------------------
------------------------------------------------
g1                             authNoPriv   internet                      -
-
------------------------------------------------------------------------------
------------------------------------------------
```

通过 **show snmp user** 查看用户和访问组的映射关系配置是否正确。

```
JX#show snmp user
User                           Group                         Auth    Priv
Filter
------------------------------------------------------------------------------
--------------------------
u1                             g1                            MD5    no-priv  N/A
------------------------------------------------------------------------------
--------------------------
```

通过 **show snmp trap-host** 查看 Trap 目标主机配置是否正确。

```
JX#show snmp trap-host
Trap-host : 192.168.62.1
------------------------------------------------------------------------------
-------
Status             : ACTIVE
Udp Port           : 162
MP Modle           : V3
Security Level      : Auth
Security Name       : u1
Vpn Instance Name    : public
------------------------------------------------------------------------------
-------
```

通过 **show snmp config** 查看所有配置信息是否正确。

```
JX#show snmp config
Software Version: SNMP_VL3.00.00.00
!
snmp server start
snmp trap-host 192.168.62.1 v3 authentication securityname u1
snmp group g1 authentication
snmp user u1 group g1 authentication md5
ACs87nMCx4RbzvvPS5lo3zDtbzu5xyzSZaDGmHOuqsc0
```

10.2 RMON

10.2.1 简介

RMON（Remote Network Monitoring，远端网络监控）是 IETF 制定的一种可以通过不同的网络代理 Agent 和网管中心进行网络数据监控的标准。

RMON 基于 SNMP 体系结构实现，包括网管中心和运行在各网络设备上的代理 Agent 两部分。在 SNMP 基础上增加了子网流量、统计、分析能力，可以实现对一个网段乃至整个网络的监控，而 SNMP 只能监控单个设备局部信息，对一个网段的监控非常困难。

RMON 中代理 Agent 一般称为探测程序，RMON Probe（RMON 探测器）能够统计和分析子网的通信性能指标，无论何时发现网络故障，RMON Probe 都能够上报网管中心，并描述不正常情况的捕获信息，网管中心无需对设备进行不停的轮询。RMON 可以比 SNMP 更主动、有效地监测远程设备，网络管理员可以更快地跟踪网络、网段或设备出现的故障。该方法减少了网管中心同代理 Agent 间的数据流量，使简单而有力地管理大型网络成为可能，弥补了 SNMP 在日益扩大的分布式互联中所面临的局限性。

RMON Probe 收集数据的方式：

- 分布式 RMON：利用专用的 RMON Probe 收集数据，网管中心直接从 RMON Probe 获取管理信息并控制网络资源。
- 嵌入式 RMON：将 RMON Agent 直接嵌入网络设备（如交换机）中，使它们成为带 RMON Probe 功能的网络设备。网管中心使用 SNMP 的基本操作与 RMON Agent 交换数据信息，收集网络管理信息。

设备采用嵌入式 RMON。如图 10-5 所示，在设备上实现了 RMON Agent 功能。通过该功能，管理站可以获得与被管网络设备接口相连的网段上的整体流量、错误统计和性能统计等信息，从而实现对一个网段的监控。

图 10-5 RMON 应用示意图

RMON MIB 中按照功能分成 9 个组，目前实现了 RMON 的四个功能组：即统计组、历史组、告警组和事件组。

- 统计组：负责收集在一个接口上的统计信息，包括接收到的报文计数和大小分布统计。
- 历史统计组：类似于统计组，但它是在一个指定的检测周期内收集统计信息。
- 告警组：在指定的时间间隔内，监视一个指定的管理信息库（MIB）对象，并且设定上升阈值和下降阈值，若监视对象达到阈值则触发一个事件。

- 事件组：配合告警组使用，当告警触发一个事件时，用来记录相应的事件信息，如发送 Trap 信息，写入日志等操作。

10.2.2 配置准备

场景

当用户需要对某一网段进行监控或流量统计时，可以配置 RMON。

RMON 是一种比 SNMP 更高效的监控手段。用户只需要指定告警阈值，超出该阈值时设备将会主动发送告警信息，而不用去获取变量信息。减少管理设备和被管理设备的通信量，对网络进行简单有效的管理。

前提

设备和网管系统之间链路可达。

10.2.3 RMON 的缺省配置

设备上 RMON 的缺省配置如下。

功能	缺省值
统计组	无
历史统计组	禁止
告警组	无
事件组	无

10.2.4 配置 RMON 统计功能

RMON 统计功能可以设置对接口的统计，包括接口收发报文、过小或过大包、冲突、循环冗余校验和错误数、丢弃报文，接收报文长度、碎片、广播、多播、单播消息等。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置节点。
2	JX(config)#**interface** *interface-type interface-number*	进入接口节点下。
3	JX(config-ge-1/0/*)#**rmon statistics** *index-number* [**owner** *owner-name*]	添加该接口的 RMON 统计功能并配置相关参数。

说明

当在接口下使用 **no rmon statistics** *index-number* 命令关闭该接口的统计功能时，是指用户不能继续获取该接口的统计数据了，而不是接口不再进行数据统计了。

10.2.5 配置 RMON 历史统计功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置节点。
2	JX(config)#**interface** *interface-type interface-number*	进入接口节点下。
2	JX(config-ge-1/0/*)#**rmon history** *index-number* **bucket** *buckets-number* **interval** *sampling-interval* [**owner** *owner-name*]	添加该接口的 RMON 历史统计功能并配置相关参数。

说明

当在接口下使用 **no rmon history** *index-number* 命令禁止该接口的历史组统计功能时，不再进行数据收集统计，并且将以前收集的所有历史数据清除。

10.2.6 配置 RMON 告警组

可通过设置 RMON 一个告警组实例（*alarm-id*），监控一个 MIB 变量（*object-id*）。当被监控数据的值越过定义的阈值时会产生告警事件，再按照告警事件的定义进行记录日志或向网管站发送 Trap 信息。

所监控的 MIB 变量必须是真实存在的，并且数据值类型设置正确。

- 如果在设置时，变量不存在或值类型不正确，则返回错误。
- 在已经设置成功的告警中，如果后期该变量无法被采集，则该告警就被关掉，若想重新监控该变量，必须重新设置。

只要事件表中配置了上限或下限其中一个事件，符合条件便会触发相应的告警。如果告警上限和下限所对应事件（*rising-event-id*、*falling-event-id*）在事件表中均没有配置，即使达到了告警条件也不会产生告警。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置节点。
2	JX(config)#**rmon alarm** *alarm-id object-id*	在 RMON 告警组中添加告警实例，并

步骤	配置	说明
	query-interval { **absolute** | **delta** } **rising-threshold** *rising-threshold rising-event* **falling-threshold** *falling-threshold falling-event* [**startup-alarm** { **rising** | **falling** | **risingorfalling** } | **owner** *owner-name*]*	配置相关参数。

10.2.7 配置 RMON 事件组

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置节点。
2	JX(config)#**rmon event** *event-id* { **log** | **trap** | **both** } [**description** *string* | **owner** *owner-name*]*	在 RMON 事件组中添加事件，并配置事件的处理方式。

10.2.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show rmon config**	查看 RMON 配置信息。
2	JX#**show rmon alarm**	查看 RMON 告警组信息。
3	JX#**show rmon event**	查看 RMON 事件组信息。
4	JX#**show rmon statistics**	查看 RMON 统计组信息。
5	JX#**show rmon history**	查看 RMON 历史统计组配置信息
6	JX#**show rmon history** *index-number*	查看指定 RMON 历史统计组信息。
7	JX#**show rmon history statistics**	查看指定 RMON 历史统计组统计信息。
8	JX#**show rmon log**	查看 RMON 事件组的日志信息。

10.2.9 维护

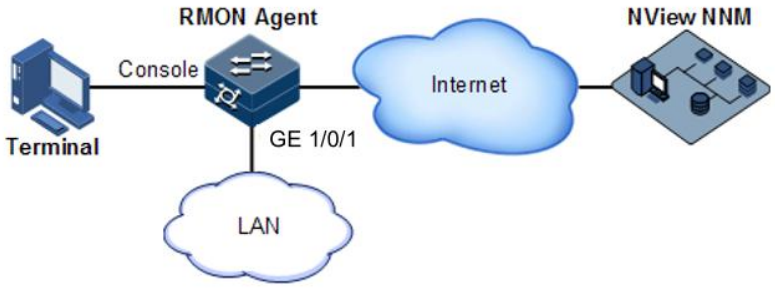
无

10.2.10 配置 RMON 告警组应用示例

组网需求

如图 10-6 所示，交换机设备作为 Agent，通过 Console 口连接配置终端，通过 Internet 连接远端 NNM 系统。使能 RMON 统计功能并对 ge 1/0/1 接口进行性能统计，当接口在一段时间内收到的报文数量超过设置的阈值后，记录日志并发送 Trap 告警。

图 10-6 RMON 典型应用组网示意图



配置步骤

步骤 1 创建索引号为 1 的事件，该事件用于记录并发送,描述字符串为 Falling-etherStatsBroadcastPkts 的日志信息，该日志信息的所有者为 **system**。

```
JX#configure
JX(config)#rmon event 1 both description Falling-etherStatsBroadcastPkts
owner system
```

步骤 2 在接口 ge 1/0/1 下创建统计表，该统计表的所有者也为 **system**

```
JX(config-ge-1/0/1)#rmon statistics 1 owner system
```

步骤 3 创建索引号为 10 的告警项，该告警项用于监控 MIB 变量 etherStatsBroadcastPkts.1 即 1.3.6.1.2.1.16.1.1.1.6.1，每 20 秒检查一次，如果该变量的取值升到 100 以上或者降到 15 以下，便触发 Trap 告警，该告警信息的所有者也为 **system**。

```
JX(config)#rmon alarm 10 1.3.6.1.2.1.16.1.1.1.6.1 20 absolute  rising-
threshold 100 1 falling-threshold 15 1 owner system
```

检查结果

通过 **show rmon alarm** 命令查看设备上是否有告警组信息。

```
JX#show rmon alarm
  RMON Alarm:10
       Interval:20
       Source OID:1.3.6.1.2.1.16.1.1.1.6.1
       Sample Type:absolute value
       Alarm Value:0
       Startup Alarm:risingOrFallingAlarm
```

```
        Rising Threshold:100
        Rising Event:1
        Falling Threshold:15
        Falling Event:1
        Owner:system
        Status:valid
```

通过 **show rmon event** 命令查看设备上是否有事件组信息。

```
JX#show rmon event
  RMON Event:1
        Type:trap&log
        Status:valid
        Lastsent time:0 days 12 hours 6 minutes 1 seconds
        Description:Falling-etherStatsBroadcastPkts
        Owner:system
```

通过 **show rmon log** 命令查看设备上是否有事件记录的日志信息。

```
JX#show rmon log
  RMON Log:1/1
        Time:0 days 12 hours 6 minutes 1 seconds
        Description:alarm falling  10,1.3.6.1.2.1.16.1.1.1.6.1,1,0,15
```

当告警事件被触发时，在 NNM 系统的告警管理部分也可以查看相应的记录。

10.3 LLDP

10.3.1 简介

随着网络规模的扩大，网络设备的增多，网络拓扑日趋复杂，对网络的管理变得尤为重要。为了跟踪网络拓扑信息的变化，许多网络管理软件都采用“自动发现”功能来跟踪网络拓扑的变化，但大多数网络管理软件只能分析到网络层拓扑结构，无法确定设备通过哪些接口与其他设备相连。

LLDP（Link Layer Discovery Protocol，链路层发现协议）是由 IEEE 802.1AB 定义的一种链路层发现协议。网络管理系统可以通过该协议快速掌握二层网络的拓扑及其变化情况。

LLDP 将本地设备的信息组织成不同的 TLV（Type Length Value，类型/长度/值单元），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发送给直连的邻居，同时将邻居发来的信息以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网管系统查询及判断链路的通信状况。

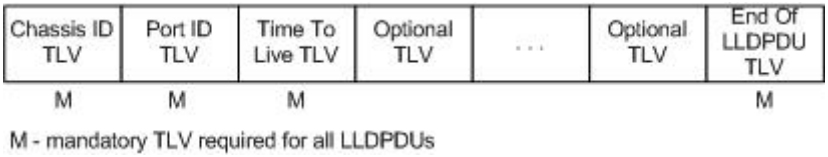
基本概念

LLDP 报文是指在数据单元封装了 LLDPDU 的以太网报文。

LLDPDU 是 LLDP 报文的数据单元。在组成 LLDPDU 之前，设备先将本地信息封装成 TLV，再由若干 TLV 组合成一个 LLDPDU，封装在以太网数据部分进行传送。

如图 10-7 所示，LLDPDU 由若干个 TLV 组合而成，其中包含四个必选的 TLV 和若干个可选的 TLV。

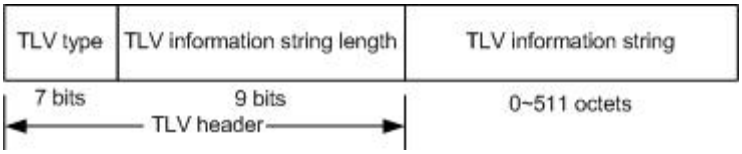
图 10-7 LLDPDU 结构图



TLV 是组成 LLDPDU 的单元，表示一个对象的类型、长度和信息的单元。

TLV 的结构如图 10-8 所示，每个 TLV 代表一个本端信息。例如设备 ID，接口 ID 等各自对应 Chassis ID TLV，Port ID TLV 固定的 TLV。

图 10-8 基本 TLV 结构图



TLV 类型值对应如表 10-1 所示，目前只用到其中的 0～8 种类型。

表 10-1 TLV 类型

TLV 类型	说明	是否必选
0	End Of LLDPDU，表示 LLDP 报文结束	必选
1	Chassis Id，发送设备的 MAC 地址	必选
2	Port Id，LLDP 报文发送端的接口	必选
3	Time To Live，本设备信息在邻居设备上的老化时间	必选
4	Port Description，以太网接口的描述信息	可选
5	System Name，设备名称	可选
6	System Description，系统描述	可选
7	System Capabilities，系统的主要功能以及已使用的功能项	可选
8	Management Address，管理地址	可选

组织定义 TLV 属于可选的 TLV 集合，根据用户的实际需要在 LLDPDU 中发布。目前比较常见的组织定义 TLV 如下。

表 10-2 IEEE 802.1 组织定义的 TLV

TLV 类型	TLV 说明
Port VLAN ID TLV	端口的 VLAN 标识符
Port And Protocol VLAN ID TLV	端口的协议 VLAN 标识符
VLAN Name TLV	端口的 VLAN 名称
Protocol Identity TLV	端口支持的协议类型

表 10-3 IEEE 802.3 组织定义的 TLV

TLV 类型	TLV 说明
MAC/PHY Configuration//Status TLV	端口的速率双工状态、是否支持并使能自动协商功能
Power Via MDI TLV	端口的供电能力
Link Aggregation TLV	端口的链路聚合能力及当前的聚合状态
Maximum Frame Size TLV	端口所能传输的最大的帧的大小

LLDP 工作原理

LLDP 是一种点对点单向发布协议，通过本机向对端周期性的发送 LLDP 报文（或者本端信息有变化时发送 LLDP 报文），通知对端本机的链路状态。

其数据流如下：

- 发送时，设备从 NMS 获取所选择 TLV 需要的系统信息，以及从 LLDP MIB 中获得配置信息，生成 TLV，组成 LLDPDU，封装成 LLDP 报文发送给对端。
- 对端接收到 LLDP 报文后，对端设备会解析获得的各个 TLV 信息，如果有变更，将信息更新至 LLDP 的邻居 MIB 表中，并通知 NMS。

本端设备信息在邻居节点中老化时间 TTL（Time to live），可通过修改老化系数参数值调整，向邻居节点发送 LLDP 报文，邻居节点收到 LLDP 报文后，调整其邻居节点（即发送端）信息的老化时间。老化时间计算公式，TTL=Min{65535，(interval×hold-multiplier)}，其中：

- interval 表示设备向邻居节点发送 LLDP 报文的时间周期。
- hold-multiplier 表示设备信息在邻居节点的老化系数。

10.3.2 配置准备

场景

当用户通过 NView NNM 系统获取设备之间的连接信息，进行拓扑发现时，需要在设备之间使能 LLDP 功能，向邻居互相通告自己的信息，以及存储邻居信息，方便 NView NNM 系统查询。

前提

无

10.3.3 LLDP 的缺省配置

设备上 LLDP 的缺省配置如下。

功能	缺省值
LLDP 全局使能或禁止	禁止
接口 LLDP 功能状态	使能
延迟发送定时器	2s
周期发送定时器	30s
老化系数	4
重启定时器	2s
告警使能或禁止	去使能
告警通知定时器	5s
LLDP 报文目的 MAC 地址	0180.c200.000e

10.3.4 使能全局 LLDP 功能

注意

禁止全局 LLDP 功能后，不能立即再使能，必须等重启定时器超时后才能再次使能。

通过 NView NNM 系统获取设备之间的连接信息，进行拓扑发现时，需要在设备之间使能 LLDP 功能，向邻居互相通告自己的信息，以及存储邻居信息，方便 NView NNM 系统查询。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**lldp { start | stop }**	使能全局 LLDP 功能，使用 stop 格式禁用该功能。 start：使能 LLDP 功能 stop：禁用 LLDP 功能

10.3.5 使能接口 LLDP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface { ge | 10ge }** *interface-number*	进入物理接口配置模式。以下步骤以物理
3	JX(config-ge-1/0/1)#**lldp admin-status { tx-only | rx-only | rx-tx | disable }** Example: JX(config-ge-1/0/1)#**lldp admin-status tx-only**	使能接口 LLDP 功能，使用 disable 格式禁用该功能。 tx-only：只发 LLDP 报文 rx-only：只收 LLDP 报文 rx-tx：收发 LLDP 报文 disable：禁用 LLDP 功能

10.3.6 全局配置 LLDP 基本功能

注意

配置延时发送定时器和周期发送定时器时，延时发送定时器的取值要小于或等于周期发送定时器取值的四分之一。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**lldp tx-interval** { <5-32768> | **default** } Example: JX(config)#**lldp tx-interval 10**	（可选）配置 LLDP 报文的周期发送定时器。 second：LLDP 报文的发送周期，整数形式，取值范围是 5～32768，单位是秒 default：2 秒

步骤	配置	说明
3	JX(config)#**lldp tx-delay** { <1-8192> | **default** } Example: JX(config)#**lldp tx-delay 5**	可选）配置 LLDP 报文的延迟发送定时器。 second：发送延迟时间，整数形式，取值范围是 1～8192，单位是秒 default：2 秒。
4	JX(config)#**lldp reinit-delay** { <1-10> | **default** } Example: JX(config)#**lldp reinit-delay 5**	可选）配置重启定时器。即设备禁止全局 LLDP 功能后，需要等待重启定时器设定的时间后才能重新使能全局 LLDP 功能。 second：重启延迟时间值，整数形式，取值范围是 1～10，单位是秒 default：2 秒
5	JX(config)#**lldp tx-hold-multiple** { <2-10> | **default** } Example: JX(config)#**lldp tx-hold-multiple 2**	（可选）配置报文发送间隔的倍数 multiple：倍数，整数形式，取值范围是 2～10，单位是倍 default：4。

10.3.7 接口配置 LLDP 基本功能

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** { **ge** | **10ge** }*interface-number* Example: JX(config)#**interface ge 1/0/1**	（可选）配置 LLDP 报文的周期发送定时器。 second：LLDP 报文的发送周期，整数形式，取值范围是 5～32768，单位是秒 default：2 秒
3	JX(config-ge-1/0/1)#**lldp management-address** { A.B.C.D } { **enable** | **disable** }	（可选）在端口下配置 LLDP 的管理地址 A.B.C.D 管理地址；Enable 使能；disable 去使能

10.3.8 配置 LLDP 告警功能

当网络自身发生变化时，需要使能 LLDP 告警通知功能，及时向 NView NNM 系统发送拓扑信息更新告警。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**lldp trap { enable | disable }**	配置 LLDP 告警 Trap 使能/去使能
3	JX(config)#**lldp trap-interval { <5-3600> | default }** Example: JX(config)#**lldp trap-interval 10**	（可选）配置 lldp 邻居变化时间通告间隔定时器 second：重启延迟时间值，整数形式，取值范围是 5～3600，单位是秒 default：5 秒

10.3.9 配置 TLV

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/1)#**lldp basic-tlv-tx { port-description | system-name | system-description | system-capability | all } { enable | disable }**	（可选）在端口下配置 LLDP 报文的基本 TLV port-description 端口描述；system-name 系统名称；system-description 系统描述；all 所有；s enable 使能；disable 去使能
4	JX(config-ge-1/0/1)#**lldp dot1-tlv- tx port-vid { enable | disable }** JX(config-ge-1/0/1)#**lldp dot1-tlv-tx protocol-vid** *vlan-list* **{ enable | disable }** JX(config-ge-1/0/1)#**lldp dot1-tlv-tx vlan-name** *vlan-list* **{ enable | disable }**	可选）配置端口下设置关于 802.1 组织定义的 TLV 的相关配置。 port-vid 端口 vlan；protocol-vid 协议 vlan；vlan-namevlan 名称；enable 使能；disable 去使能
5	JX(config-ge-1/0/1)#**lldp dot3-tlv-tx { mac-phy | power | link-aggregation | max-frame-size | all } { enable | disable }**	（可选）配置端口下关于 802.3 组织定义的 TLV 的相关配置 mac-phy 端口的速率；power 端口的供电能力；link-aggregation 链路聚合；max-frame-size 最大帧长度；all 所有；enable 使能；disable 去使能

步骤	配置	说明
6	JX(config-ge-1/0/1)#**lldp med-tlv- tx { capabilities | network-policy | location | extended-pse | extended-pd | inventory | all } { enable | disable }**	（可选）配置端口下与 MED 相关的配置 Capabilities 能力级；network-policy 支持的应用；location 端口位置标识信息；extended-pse 供电能力；extended-pd 供电能力；inventory 详细目录； all 所有；enable 使能；disable 去使能
7	JX(config-ge-1/0/1)# **lldp voice-vlan { untagged | vlan** *vlan-id* **[cos {***cos-value* **| default} | dscp {***dscp-value* **| default}] }**	（可选）配置端口下与 network-policy tlv 封装 voice vlan 相关的配置 Untagged 配置终端设备发送语音流量时不带 VLAN ID；vlan-id 配置 voice-vlan 的 VLAN ID；cos-value 配置 CoS 优先级，默认值为 5；dscp-value 配置 DSCP 优先级，默认值为 46

10.3.10 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX# **show lldp config**	显示 lldp 配置
2	JX#**show lldp information**	查看 LLDP 本地系统信息。
3	JX#**show lldp remote** [*interface-type interface-number*]	查看 LLDP 邻居信息。
4	JX#**show lldp statistics** [*interface-type interface-number*]	查看 LLDP 报文统计信息。
5	JX#**show lldp interface** [*interface-type interface-number*]	查看 LLDP 端口信息。

10.3.11 维护

用户可以通过以下命令维护 LLDP 特性。

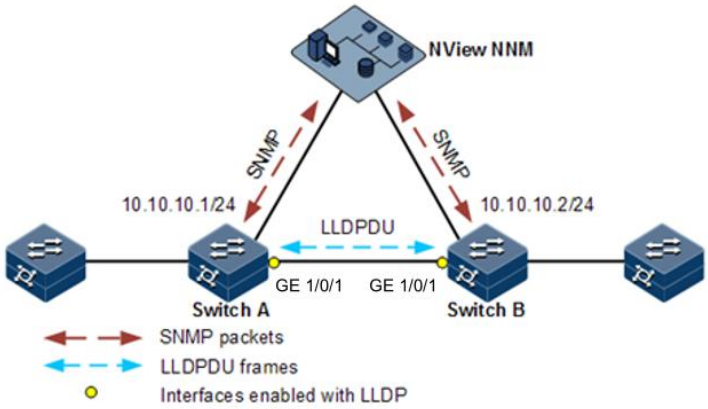
命令	说明
JX(config-ge-1/0/1)#**reset lldp port statistics**	接口下清除 LLDP 统计信息。

10.3.12 配置 LLDP 基本功能示例

组网需求

如图 10-9 所示，交换机和 NView NNM 系统相连，在 Switch A 和 Switch B 之间使能 LLDP 协议，则两设备之间二层链路的变化情况，可以通过 NView NNM 系统查询。如果邻居老化、新增邻居、邻居信息变化时会向 NView NNM 系统上报 LLDP 告警。

图 10-9 配置 LLDP 基本功能组网示意图



配置步骤

步骤 1 配置全局使能 LLDP 并使能 LLDP 告警。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#lldp start
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#config
SwitchB(config)#lldp start
```

步骤 2 配置管理 IP 地址。

配置 Switch A。

```
SwitchA(config)# vlan 10
SwitchA(config)# interface vlan 10
SwitchA(config)# interface GE 1/0/1
SwitchA(config-ge-1/0/1)# port hybrid vlan 10 tagged
SwitchA(config-ge-1/0/1)# port hybrid pvid 10
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface vlan 10
```

```
SwitchA(config-vlan1024)# ip address 10.0.0.1/24
SwitchA(config-vlan1024)#exit
```

配置 Switch B。

```
SwitchB(config)# vlan 10
SwitchB (config)# interface vlan 10
SwitchB (config)# interface GE 1/0/1
SwitchB (config-ge-1/0/1)# port hybrid vlan 10 tagged
SwitchB (config-ge-1/0/1)# port hybrid pvid 10
SwitchB (config-ge-1/0/1)#exit
SwitchB (config)#interface vlan 10
SwitchB (config-vlan1024)# ip address 10.0.0.2/24
SwitchB (config-vlan1024)#exit
```

步骤 3 配置 LLDP 属性。

配置 Switch A。

```
SwitchA(config)# lldp tx-interval 60
SwitchA(config)# lldp tx-delay 9
SwitchA(config)# lldp trap-interval 10
```

配置 Switch B。

```
SwitchA(config)# lldp tx-interval 60
SwitchA(config)# lldp tx-delay 9
SwitchA(config)# lldp trap-interval 10
```

检查结果

通过 **show lldp information** 命令查看本地配置是否正确。

```
SwitchA#show lldp information
  LLDP local:
       Message tx-interval:60(s)
       Message tx-hold:4
       Reinit delay:2(s)
       Tx delay:9(s)
       Notification interval:10(s)
       Chassis type:MAC Address
       Chassis ID:f0f1:f2f3:0101
       System name:SIM-MPU
       System desc:SWITCH
       System supported:Bridge/Switch,Router
       System capenabled:Bridge/Switch,Router

    Port ge-1/0/1:
       Admin status:TxRx
       Trap enable:no
       Support tlv:port-description,system-name,system-description,system-
capability
       Enabled tlv:port-description,system-name,system-description,system-
capability
       Port type:interface name
       Port ID:GE1/0/1
       Port description:GE1/0/1 SNMP-Index:537397249
```

```
        Number of remote system:1
        Number of MED remote system:0
……
```

通过 **show lldp remote** 命令查看邻居信息是否建立。

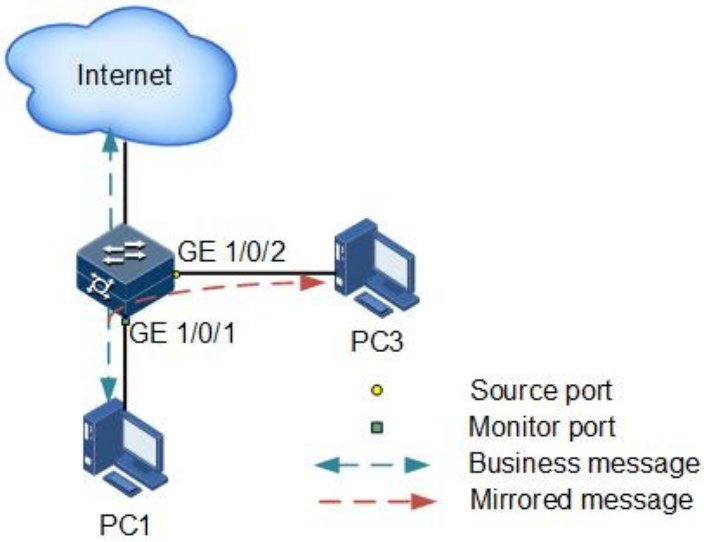
```
SwitchA#show lldp remote
Interface      Index TTL(s)  ChassId                    PortId
 SysName Vlan
ge-1/0/1       1     116     f0f1:f2f3:0201             GE1/0/1
 SIM-MPU 10
ge-1/0/2       2     116     f0f1:f2f3:0201             GE1/0/2
 SIM-MPU --
……
```

10.4 端口镜像

10.4.1 简介

接口镜像功能是指将指定源接口的某些报文镜像到目的接口，即监视接口，而不影响正常报文转发的功能。交换机设备用户使用该功能可以监控某个接口的报文接收和发送情况，并分析相关网络状况。

图 10-10 接口镜像功能原理示意图



接口镜像功能基本原理如上图所示。PC 1 通过交换机的 GE 1/0/1 与外网连接，PC 3 为监测 PC，通过交换机的 GE 1/0/2 与外网连接。

当要监测从 PC 1 发出的报文时，需要将 PC 1 所连接设备的 GE 1/0/1 指定为镜像源接口，并使能对入接口报文的镜像功能，而将 GE 1/0/2 指定为监视接口，即镜像目的接口。

当 GE 1/0/1 发出的业务报文进入交换机时，交换机将对入报文进行转发，并复制一份到监视接口（GE 1/0/2）。连接在监视接口的监控设备可以接收这些被镜像的报文，并进行相关的分析工作。

设备支持基于入接口和出接口的数据流镜像。镜像功能生效后，出/入镜像接口的报文会被复制一份到监视接口。监视接口与镜像接口不能为同一个接口。

10.4.2 配置准备

场景

接口镜像功能主要用在网络管理人员定期监控网络内数据类型及流量。

接口镜像功能是将需要被监控接口的流量复制到一个监视接口或者 CPU，从而抓取入/出接口出现故障或异常时的数据流，用来分析、发现问题根源并及时解决。

前提

无

10.4.3 接口镜像的缺省配置

设备上接口镜像的缺省配置如下。

功能	缺省值
接口镜像功能状态	禁止
镜像源接口	无

10.4.4 配置接口镜像功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**mirror group** group-number *interface-type interface-number* { **rspan** *vlan-id* **tpid** { **standard** | protocol-id } }	group-number：指定镜像组号 取值范围是 1~4 interface-type：接口类型 interface-number：接口号为 unit/slot/port 形式，取值范围由接口类型决定 （可选）vlan-id：指定远程镜像 VLAN ID 取值范围是 1~4094 （可选）standard ：指定为标准值 0x8100 （可选）protocol-id：当前接口的外层 Tag 的标签协议标识 取值范围是 <0x0-0xffff>。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式
4	JX(config-ge-1/0/1)#**mirror** { **inbound** | **outbound** | **both** } **group** *group-number*	配置接口镜像规则 { ingress | egress | both }：指定镜像方向，入方向、出方向、入/出同时 group-number：指定镜像组号 取值范围是 1~4。

10.4.5 VLAN 镜像的缺省配置

设备上接口镜像的缺省配置如下。

功能	缺省值
VLAN 镜像功能状态	禁止
镜像源接口	无

10.4.6 配置 VLAN 镜像功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**mirror group** group-number *interface-type interface-number* { **rspan** *vlan-id* **tpid** { **standard** | *protocol-id* } }	group-number：指定镜像组号 取值范围是 1~4 interface-type：接口类型 interface-number：接口号为 unit/slot/port 形式，取值范围由接口类型决定 （可选）vlan-id：指定远程镜像 VLAN ID 取值范围是 1~4094 （可选）standard ：指定为标准值 0x8100 （可选）protocol-id：当前接口的外层 Tag 的标签协议标识 取值范围是 <0x0-0xffff>。
3	JX(config)#vlan *vlan-id*	进入 VLAN 接口配置模式
4	JX(config-vlan-*)#**mirror** { **inbound** | **outbound** | **both** } **group** *group-number*	配置接口镜像规则 { ingress | egress | both }：指定镜像方向，入方向、出方向、入/出同时 group-number：指定镜像组号 取值范围是 1~4。

注意

- 开启远程接口镜像时，需要在设备上关闭远程镜像 VLAN 的 MAC 地址学习功能，以保证镜像功能的正常进行。
- 确保源设备与目的设备之间的镜像报文可以二层转发，中间设备连接到源设备和目的设备方向的端口上需允许远程镜像 VLAN 通过。
- 配置镜像源接口时，不能将源端口加入到远程镜像 VLAN 中，否则会影响镜像功能的正常使用。
- 创建远程镜像 VLAN 不能作为业务 VLAN 使用，否则会影响镜像功能的正常使用。

10.4.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show mirror group**	显示镜像组配置信息。
2	JX#**show mirror interface**	显示接口上的镜像配置信息

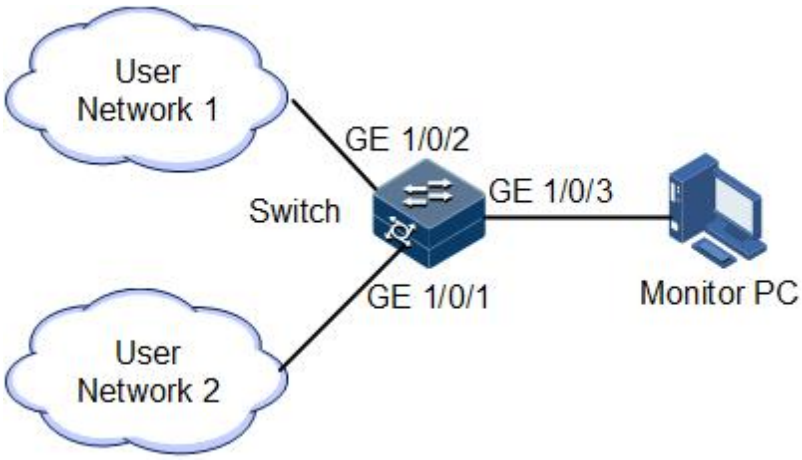
10.4.8 配置接口镜像应用示例

组网需求

如下图所示，网络管理员希望通过数据监测设备仅对用户网络 1 的报文进行监控，从而抓取出现故障或异常时的数据流，来分析、发现问题根源并及时解决。

交换机禁止所有自发包功能和风暴抑制功能。用户网络 1 通过 GE 1/0/2 接入交换机；用户网络 2 通过 GE 1/0/1 接入交换机；数据监测设备连接在交换机的 GE 1/0/3 上。

图 10-11 接口镜像应用组网示意图



配置步骤

步骤 1 在 Switch 上使能接口镜像功能。

```
JX#config
JX(config)#mirror group 1 ge 1/0/3
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#mirror inbound group 1
```

检查结果

通过 **show mirror** 查看接口镜像信息配置是否正确。

```
JX#show mirror group
Group      Observe-port     Rspan(vlan/tpid)
------------------------------------------------------------------------
  1         ge-1/0/3         n/a
------------------------------------------------------------------------
```

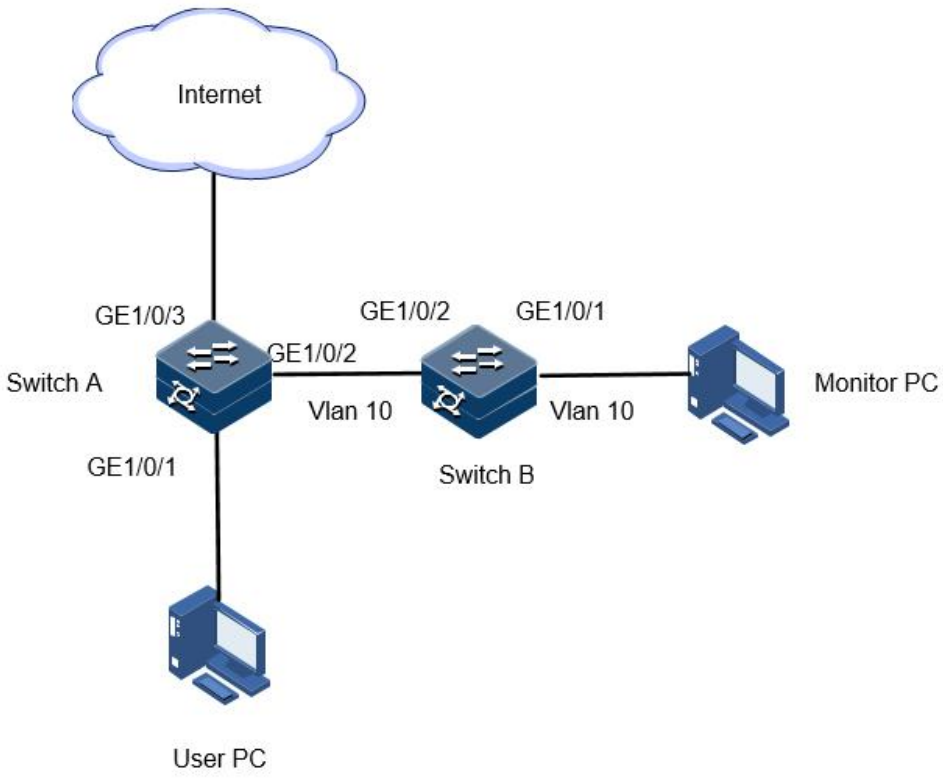
10.4.9 配置远端接口镜像应用示例

组网需求

如下图所示，网络管理员希望通过远端数据监测设备仅对用户 PC 的报文进行监控，从而抓取出现故障或异常时的数据流，来分析、发现问题根源并及时解决。

交换机禁止所有自发包功能和风暴抑制功能。用户通过 GE 1/0/1 接入 switch A；数据监测设备连接在 switch B 的 GE 1/0/1 上。

图 10-12 接口远端镜像应用组网示意图



配置步骤

步骤 1 在 Switch A 上使能接口镜像功能。

```
JX#config
JX(config)#mirror group 1 ge 1/0/2 rspan 10 tpid 0x8100
JX(config)#interface ge 1/0/1
JX(config-gigaethernet1/0/1)#mirror inbound group 1
```

步骤 2 在 Switch B 上配置 VLAN 转发。

```
JX#config
```

```
JX(config)#interface ge 1/0/1
JX(config-gigaethernet1/0/1)#port trunk allow-pass vlan 10
JX(config)#interface ge 1/0/2
JX(config-gigaethernet1/0/2)#port trunk allow-pass vlan 10
```

10.5 电缆诊断

10.5.1 简介

设备支持电缆诊断功能，可以对线路进行检测。

电缆诊断可查询的结果如下：

- 发送线缆的检测结果；
- 发送线缆的错误位置；
- 接收线缆的检测结果；
- 接收线缆的错误位置。

10.5.2 配置准备

场景

使能设备的电缆诊断功能，可及时了解设备电缆线路的运行状态，及早定位并排除设备电缆故障。

前提

无

10.5.3 配置电缆诊断功能

请在需要配置电缆诊断的设备上进行以下配置。

步骤	配置	说明
1	JX(config)#**virtual-cable-test force-detect**	全局使能电缆诊断，对设备上所有支持电缆诊断的端口进行一次电缆诊断。
2	JX(config-ge-1/0/5)#**virtual-cable-test**	使能接口的电缆诊断功能。

说明

使能接口电缆诊断不重启接口的功能时，如果接口状态为 Up，接口会重启一次，获取电缆诊断数据。配置此功能后，执行电缆诊断时，如果接口状态为 Up，接口不会再次重启，直接读取缓存中上次电缆诊断的数据；如果接口状态为 Down，接口执行一次实际电缆诊断获取实际故障点的长度；新插入的接口会自动执行电缆诊断并将结果存入缓存。

10.5.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX(config)#**show virtual-cable-test config**	查看电缆诊断相关配置信息。
2	JX(config)#**show virtual-cable-test**	查看所有接口的电缆诊断的结果。
3	JX(config)#**show virtual-cable-test interface** *interface-type primary-interface-number*	查看指定接口的电缆诊断的结果。
4	JX(config)#**show virtual-cable-test link-down**	查看所有是 down 状态接口的电缆诊断的结果。

10.6 UDLD

10.6.1 简介

UDLD（UniDirectional Link Detection，单向链路检测）用于监听利用光纤或以太网线连接的物理配置，当出现单向链路（只能向一个方向传输）时，UDLD 可以检测出这一状况，关闭相应接口并发送警告信息。单向链路可能引起很多问题，尤其是生成树，可能会造成回环。

10.6.2 配置准备

场景

当出现单向链路（只能向一个方向传输）时，UDLD 可以检测出这一状况，关闭相应接口并发送警告信息。

原理

UDLD 协议通过与对方交互协议报文（DLDPDU）来识别对端设备、检测单向链路。UDLD 协议有七种状态：Init（初始化）、Linkdown（未连通）、Linkup（活动）、Advertisement（通告）、Detect（探测）和 Disable（单通）状态。

前提

UDLD 需要链路两端设备都支持才能正常运行。

10.6.3 UDLD 功能的缺省配置

设备上故障转移功能的缺省配置如下。

功能	缺省值
UDLD 功能	禁用

10.6.4 配置 UDLD

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局模式。
2	JX(config)#**udld error-down recovery** { **disable** | **enable** }	配置单向链路恢复使能或去使能。
3	JX(config)#**udld error-down recovery-interval** *interval*	配置单向链路恢复时间间隔，默认值为 45 秒。
4	JX(config)#**udld work-mode** { **aggressive** | **normal** }	配置 UDLD 协议工作模式，分为普通模式和激进模式。
5	JX(config)#**udld advertise-interval** *interval*	配置 UDLD 协议发送 advertise 报文事件间隔，默认事件间隔为 7 秒。
6	JX(config)#**udld default-up-delay** { *time* | **default** }	配置全局的端口单通恢复时端口延迟 up 的时间。
7	JX(config)#**udld snmp-trap** { **disable** | **enable** }	使能或去使能 UDLD 协议发送 TRAP 功能。
8	JX(config)#**udld unidirection-shutdown** { **auto** | **manual** }	配置当 UDLD 协议检测到端口单通时是自动还是自动将端口关闭。
9	JX(config)#**interface** *interface-type primary-interface-number* JX(config-ge-1/0/*)#**udld** { **disable** | **enable** }	端口下使能或去使能 UDLD 功能。
10	JX(config-ge-1/0/*)#**udld aggressive** { **disable** | **enable** }	使能或去使能端口的 UDLD 协议工作模式为激进模式。
12	JX(config-ge-1/0/*)#**udld rx-mode** { **normal** | **rxloss** }	配置端口是否关注光模块 RXLOS 等相关消息进而进行接口 error-down 和 up 处理。
13	JX(config-ge-1/0/*)#**udld up-delay** *time*	配置端口的单通恢复时端口延迟 up 的时间。

10.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show udld config	查看 UDLD 配置信息。
2	JX#show udld interface	查看所有使能了 UDLD 协议的端口的协议状态
3	JX#show udld local	查看 UDLD 协议本地信息。
4	JX#show udld peer	查看 UDLD 协议邻居信息。

10.7 光模块数字诊断

10.7.1 简介

设备上光模块数字诊断支持对 SFP（Small Form-factor Pluggables，小型封装可插拔）光模块的诊断。

光模块数字诊断功能为系统提供一种性能监测手段，网络管理员通过分析该模块提供的监测数据，可以预测收发模块的寿命、隔离系统故障并在现场安装中验证模块的兼容性。

光模块数字诊断功能监控光模块的性能参数包括：

- 模块温度
- 内部供电电压
- 发送偏置电流
- 发送光功率
- 接收光功率

当性能参数达到了告警阈值或状态信息发生变化，会产生相应的 Trap 告警信息。

10.7.2 配置准备

场景

光模块故障诊断功能为用户提供一种对 SFP 光模块性能参数的检测手段，用户通过分析光模块的监测数据，可以预测其寿命、隔离系统故障并在现场安装中验证光模块的兼容性。

前提

设备所使用光模块要求为甲信认证光模块，如使用其他厂家光模块，可能导致业务不稳定、不支持诊断或诊断信息不准确等问题。

10.7.3 光模块数字诊断的缺省配置

设备上光模块数字诊断的缺省配置如下。

功能	缺省值
接口光模块数字诊断告警发送 Trap 功能	禁止

10.7.4 配置使能光模块数字诊断

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**transceiver monitor interval** *interval*	配置光模块数字诊断轮询间隔时间。

10.7.5 配置光模块数字诊断告警发送 Trap

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	JX(config 10ge 1/0/*)#**transceiver snmp-trap** { **enable** | **disable** }	使能接口光模块数字诊断告警发送 Trap。
4	JX(config 10ge 1/0/*)#**transceive rx-power low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*	设置光模块收光功率的高低门限值，在光模块收光功率低于低门限值或者高于高门限值时，光模块可以发出相应告警
5	JX(config 10ge 1/0/*)#**transceive tx-power low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*	设置光模块发光功率的高低门限值，在光模块发光功率低于低门限值或者高于高门限值时，光模块可以发出相应告警
6	JX(config 10ge 1/0/*)#**transceive temperature low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*	设置光模块温度的高低门限值，在光模块温度低于低门限值或者高于高门限值时，光模块可以发出相应告警
7	JX(config 10ge 1/0/*)#**transceive voltage low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*	设置光模块电压的高低门限值，在光模块电压低于低门限值或者高于高门限值时，光模块可以发出相应告警

步骤	配置	说明
8	JX(config 10ge 1/0/*)#**transceive bias-current low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*	设置光模块偏执电流的高低门限值，在光模块偏执电流低于低门限值或者高于高门限值时，光模块可以发出相应告警
9	JX(config 10ge 1/0/*)#**transceive tec-current low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*	设置光模块制冷电流的高低门限值，在光模块制冷电流低于低门限值或者高于高门限值时，光模块可以发出相应告警

10.7.6 检查配置

配置完成后，请在设备上进行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show transceiver config**	查看当前配置的光模块监控信息的相关配置。
2	JX#**show transceiver interface**	查看光模块的大概数字诊断信息，展示光模块的收发光功率、温度、电压、偏执电流等实时信息。
3	JX#**show transceiver** *interface-type primary-interface-number*	查看指定端口的光模块的相关监控信息。
4	JX#**show transceiver** *interface-type primary-interface-number* **threshold**	查看指定端口上配置的光模块相关监控信息的门限值。

10.8 系统日志

10.8.1 简介

系统日志功能是指设备将系统信息和调试信息等内容以日志的形式记录并输出到指定的目的地，在设备发生故障时，方便用户查看和定位故障。

设备的系统消息和一些调试输出会被送至系统日志处理。系统日志根据用户的配置将信息送往不同的目的地，接收系统日志的目的地有以下几类。

- Console 控制台：将日志信息通过 Console 接口输出到本地控制台。
- Monitor 监控台：将日志信息输出到监控台，如 Telnet 终端。
- Logfile 日志文件：将日志信息以日志文件形式输出到设备的 Flash 中。
- Buffer 缓冲区：将日志信息输出到 log 缓冲区中。
- Trapbuffer 缓冲区：将日志信息输出到 trap 缓冲区中。

- SNMP 服务器：将日志信息转化为 Trap 输出到 SNMP 服务器。
- Syslog 服务器：将日志信息输出到 syslog 服务器。
- Smtp 电子邮件：将日志信息输出到 smtp 电子邮件。

系统日志信息级别，根据严重程度分为 8 个等级，如表 10-4 所示。

表 10-4 信息级别

严重等级	级别	说明
emergencies	0	系统不可以使用
alerts	1	需要立即处理
critical	2	严重状态
error	3	错误状态
warning	4	警告状态
notification	5	正常但是很重要的状态
information	6	通告事件
debugging	7	调试信息

说明

输出信息的严重等级是可手动设置的。根据配置的严重等级输出信息时，仅输出级别小于或等于所配置的严重等级的信息。比如，配置输出级别指定为 3（也可直接指定严重等级 error）的信息输出，则级别为 0～3 的信息，即严重等级为 emergencies～error 的信息均可以输出。

10.8.2 配置准备

场景

设备会将系统的登录成功失败、关键信息、调试信息、错误信息等生成系统日志，输出为日志文件或传送到日志主机、Console 接口或监控台，以便用户查看并定位故障。

前提

无

10.8.3 系统日志的缺省配置

设备上系统日志的缺省配置如下。

功能	缺省值
系统日志功能状态	使能
日志消息输出到 console 控制台功能	使能，缺省级别为 warning（4）
日志信息输出到 file 文件功能	使能，缺省级别为 debugging(7)
日志输出到 monitor 监控台功能	使能，缺省级别为 warning（4）
日志输出到 buffer 缓冲区功能	使能，缺省级别为 debugging（7）
日志输出到 SNMP 服务器功能	禁止，缺省级别为 debugging（7）
日志输出到 Trapbuffer 缓冲区功能	禁止，缺省级别为 information（6）
日志输出到 syslog 服务器功能	禁止，缺省级别为 information（6）
日志输出到 smtp 电子邮件功能	禁止，缺省级别为 warning（4）

10.8.4 配置系统日志基本信息

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**logging** { start | **stop** }	配置使能系统日志功能。
3	JX(config)#**logging file max-number** { *max-num* | **default** }	配置系统日志的日志文件最大个数。
4	JX(config)#**logging file size kbytes** { *size-value* | **default** }	配置系统日志的日志文件大小。

10.8.5 配置系统日志输出

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**logging module** *module-name* **action** { **console** | **monitor**|**logfile** | **buffer** | **trap** | **trapbuffer** | **syslog** | **smtp** } { **log** | **debug** | **trap** } [**state** { **enable** | **disable** | **default** } | **level** { **emergencies** | **alert** | **critical** | **error** | **warning** | **notification** | **information** | **debugging** | **default** }	配置模块日志输出方向，输出使能以及输出级别

10.8.6 配置系统日志输出 TELNET/SSH 终端

步骤	配置	说明
1	JX#terminal monitor JX#no terminal monitor	打开关闭信息输出到 TELNET/SSH 终端。
2	JX#terminal log JX#no terminal log	打开关闭日志信息输出到 TELNET/SSH 终端。缺省为开启状态。
3	JX#terminal trap JX#no terminal trap	打开关闭 Trap 信息输出到 TELNET/SSH 终端。缺省为开启状态。
4	JX#terminal debug JX#no terminal debug	打开关闭 Trap 信息输出到 TELNET/SSH 终端。缺省为关闭状态。

10.8.7 检查配置

在设备上执行以下命令可以查看日志相关信息与配置。

序号	检查项	说明
1	JX#show logging information	查看日志配置的全局信息。
2	JX#show logging { buffer | trap }	查看日志或者 trap 缓冲区信息。
3	JX#show logging { buffer | trap } { include | exclude | begin } string *STRING*	查看日志或者 trap 缓冲区信息，指定字符串过滤条件。
4	JX#show logging { buffer | trap } size *size-number*	查看日志或者 trap 缓冲区信息，指定条目数。
5	JX#show logging { buffer | trap } module *module-name*	查看指定模块的日志或者 trap 缓冲区信息。
6	JX#show logging { buffer | trap } size *size-number* { include | exclude | begin } string *string*	查看日志或者 trap 缓冲区信息，指定条目数和字符串过滤条件。
7	JX#show logging { buffer | trap } start-time *start-time* [end-time *end-time*]	查看日志或者 trap 缓冲区信息，指定日志产生的时间范围。
8	JX#show logging action	查看日志所有模块的动作信息。
9	JX#show logging action { console | monitor|logfile | buffer | trap | trapbuffer | syslog | smtp }	查看日志所有模块指定动作信息。
10	JX#show logging error	查看所有模块日志的错误码信息。
11	JX#show logging event	查看所有模块日志的事件信息。

序号	检查项	说明
12	JX#**show logging file** *file-name*	查看指定日志文件的内容
13	JX#**show logging file** *file-name* { **include** | **exclude** | **begin** } **string** *string*	查看指定日志文件的指定内容，指定字符串过滤条件。
14	JX#**show logging module**	查看所有模块日志的信息，包括模块名、模块 ID、日志文件名、事件数目和错误码条目数。
15	JX#**show logging statistics**	查看日志模块的统计信息。

10.8.8 维护

用户可以通过以下命令，维护系统日志特性的运行情况和配置情况。

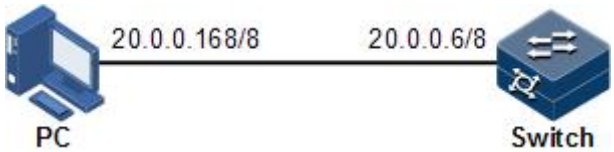
命令	描述
JX(config)#**clear logging** { **buffer** | **trap** }	清除 log 或者 trap 缓冲区中的日志信息。
JX(config)#**clear logging statistics**	清除日志的统计信息。
JX(config)#**clear logging file all**	清除所有日志文件。
JX(config)#**clear logging module** *module-name*	清除指定模块日志的统计信息。

10.8.9 配置系统日志输出到当前终端示例

组网需求

如图 10-13 所示，配置系统日志功能，将设备上的日志信息输出到日志主机，以便用户随时查看。

图 10-13 系统日志输出到日志主机组网示意图



配置步骤

步骤 1 配置设备的 IP 地址。

```
JX#configure
JX(config)#interface vlan 1
```

```
JX(config-vlanif-1)#ip address 20.0.0.6 255.0.0.0
JX(config-vlanif-1)#quit
```

步骤 2 配置系统日志输出到终端上。

```
JX(config)#terminal monitor
```

步骤 3 配置调试信息输出到终端上。

```
JX(config)#terminal debug
```

检查结果

通过 **show logging information** 命令查看系统日志全局配置信息是否正确。

```
JX#show logging information
-------------------------------------------------------------
  Logging                : on
  Module number           : 125
  Logfile path            : "/ram/log"
  Logfile max size         : 3072 Kb
  Logfile max number       : 3
  Logbuffer Max number     : 2000
  Logbuffer Current number : 201
  Logbuffer history number : 216
-------------------------------------------------------------
```

10.9 告警管理

10.9.1 简介

告警是指当设备出现故障或某些工作状态发生变化时，系统能够根据不同故障类型、不同告警来源产生的信息。

告警信息用于报告一些紧急且重要的事件，及时通知网络管理人员，为监控设备运行和进行故障诊断提供有力支持。

告警信息保存在设备的告警缓存区中，同时将生成日志信息。若配置了网管系统，则该告警信息会通过 SNMP 向网管系统发送，发送给网管系统的信息称为 Trap 信息。

10.9.2 配置准备

场景

设备发生故障时，由告警管理模块来收集设备故障信息，以日志等形式输出告警的发生时间、告警的名称和描述信息等，帮助用户快速进行问题定位。

如果设备上配置网管系统，告警信息可以直接上报网管系统，给出告警产生的可能原因和处理建议，帮助用户及时处理故障。

如果设备上配置了硬件监控功能。当设备运行环境出现异常时，会记录硬件监控告警表、产生 Syslog 系统日志或发送 Trap 等告警信息，通知用户进行相应处理，防止故障发生。

告警管理方便用户直接在设备上进行告警抑制，告警自动上报，告警监控，告警反转，告警延迟，告警存储模式，清除告警，查看告警等配置。

前提

如果设备上需要配置硬件监控功能时：

- 以 Syslog 方式输出时，告警信息会生成系统日志。当需要把告警信息发送到系统日志主机时，设备上需要配置系统日志主机的 IP 地址等信息。
- 需要把告警信息以 Trap 方式发送到网管中心时，设备上需要配置网管中心的 IP 地址等信息。

10.9.3 配置告警基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

10.9.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show alarm information**	查看告警管理模块的表项数量信息。
2	JX#**show alarm description**	查看告警管理模块的所有告警信息。 包括告警 id、告警名称、告警级别、对应 Trap-OID 和描述信息。
3	JX#**show alarm** { **active** | **history** | **all** } **time-order** [**object** *object-name*]	查看指定告警信息，并且按时序排列（活动告警、历史告警、全部告警）。
4	JX#**show alarm** { **active** | **history** | **all** } [**object** *object-name*]	查看指定告警信息（活动告警、历史告警、全部告警）。
6	JX#**show alarm object**	查看告警对象信息。
7	JX#**show event description**	查看告警管理模块的所有事件信息。 包括事件 id、事件名称、事件级别、对应 Trap-OID 和描述信息。
8	JX#**show event all** [**object** *object-name*]	查看告警管理模块的所有当前事件。

10.10 CPU 监控

10.10.1 简介

设备支持 CPU 监控功能，可以实时监控系统中各任务的状态、CPU 利用率和堆栈使用情况，帮助网管人员快速定位故障。

CPU 监控可以提供以下功能：

- 查看 CPU 利用率

提供查看各周期（5 秒，1 分钟，5 分钟）内各任务的 CPU 利用率，可以静态显示。

提供查看所有任务的运行状态信息。

- CPU 利用率门限告警

在指定的采样周期内，系统的 CPU 利用率从低于下限阈值上升到高于上限阈值或者从高于上限阈值下降到低于下限阈值时，会产生告警并发送 Trap，Trap 信息会提供最近某个周期（5 秒，1 分钟，5 分钟）内 CPU 利用率最高的 5 个任务序号及其 CPU 利用率。

10.10.2 配置准备

场景

CPU 监控功能可以实时监控系统中各任务的状态、CPU 利用率和堆栈使用情况，提供 CPU 利用率门限值告警，方便及时发现并消除隐患，或帮助网管人员进行故障定位。

前提

在配置 CPU 监控之前，需完成以下任务：

- 当需要把 CPU 监控告警信息以 Trap 方式输出时，需在设备上配置 Trap 输出目标主机地址，即网管中心的 IP 地址等信息。

10.10.3 CPU 监控的缺省配置

设备上 CPU 监控的缺省配置如下。

功能	缺省值
CPU 利用率告警 Trap 输出	使能
CPU 利用率告警的上限阈值	80%
CPU 利用率采样周期	10s

10.10.4 配置 CPU 监控告警

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**cpu { all** | *cpu-index* **} high-threshold** *high-threshold-value*	设置所有 CPU 表项或指定 CPU 表项的告警的上限阈值。
3	JX(config)#**cpu { all** | *cpu-index* **} description** *description-string*	设置所有 CPU 表项或指定 CPU 表项的描述信息。
4	JX(config)#**cpu { all** | *cpu-index* **} snmp-trap { disable** | **enable }**	设置所有 CPU 表项或指定 CPU 表项的发送 TRAP 使能或去使能。
5	JX(config)#**cpu monitor interval** *interval-value*	配置 CPU 利用率采样时间间隔。
6	JX(config)#**cpu monitor { disable** | **enable }**	使能或去使能 CPU 利用率监控。

10.10.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show cpu**	查看 CPU 利用率。
2	JX#**show cpu verbose**	查看 CPU 利用率的相关详细信息。
3	JX#**show cpu task**	查看各任务的 CPU 利用率。

10.11 内存监控

10.11.1 配置准备

场景

内存利用率监控功能可以实时监控系统的内存利用率，提供内存利用率阈值告警，方便及时发现并消除隐患，或帮助网管人员进行故障定位。

前提

当用户需要把内存利用率监控告警信息以 Trap 方式输出时，应首先在设备上配置 Trap 输出目标主机地址，即网管中心的 IP 地址等信息。

10.11.2 配置内存监控

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**memory { all** | *memory-index* **} high-threshold** *high-threshold-value*	配置所有内存表项或者指定内存表项的监控告警门限阈值。
3	JX(config)#**memory { all** | *memory-index* **} description** *description-string*	配置所有内存表项或者指定内存表项的描述信息。
4	JX(config)#**memory { all** | *memory-index* **} snmp-trap { disable** | **enable }**	配置所有内存表项或者指定内存表项的 TRAP 使能或去使能。
5	JX(config)#**memory monitor interval** *interval-value*	配置内存利用率的监控周期。
6	JX(config)#**memory monitor { disable** | **enable }**	配置内存利用率监控使能或去使能。

10.11.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show memory**	查看系统内存利用率。
2	JX#**show memory verbose**	查看系统内存利用率的详细信息。
4	JX#**show memory task**	查看系统内每个进程的内存占用信息。

10.12 Ping

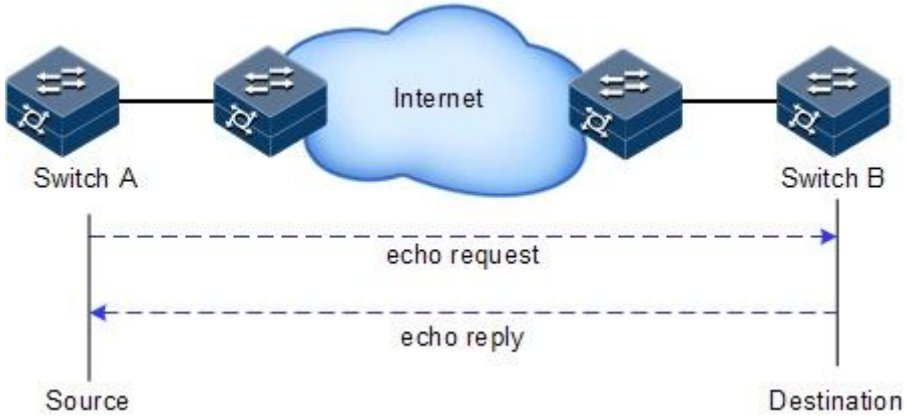
10.12.1 简介

Ping 的名字源于声纳定位操作，用于检测网络连接是否正常。

Ping 功能一般借助 ICMP echo 报文来实现。首先发送 echo request 报文到某个地址，然后等待该地址对应的设备响应 echo reply 报文，当 echo request 到达目标地址以后，在一个有效的时间内返回 echo reply 报文给源地址，则说明目的地可达。如在有效时间内没有收到回应，则在发送端显示超时，并表明目的地不可达。

Ping 功能实现原理如图 10-14 所示。

图 10-14 Ping 功能实现原理组网示意图



10.12.2 配置 Ping 功能

请在设备上进行以下操作。

步骤	配置	说明
1	JX#**ping** { *ipv4-address* | *hostname* } [**-n** *nvalue*|**-system-time**|**-t**|**-q**|**-f**|**-h** *hvalue*|**-l** *lengthvalue*|**-w** *waitvalue*|**-tos** *tosvalue*|**-m** *mvalue*|**-dscp** *dscpvalue*|**-8021p** *8021pvalue*|**-range** *rangevalue*|**-s** *source-ipv4-address*|**-nexthop** *next-ipv4-address*|**-eth-trunk** *trunk-number*|**-loopback** *loopback-number*|**-vlan** *vlan-id*|**-ge** *interface-number1*|**-10ge** *interface-number2*|**-meth** *meth-number*]	通过 **ping** 命令测试 IPv4 网络的连通性。
2	JX#**ping-ipv6** {*ipv6-address*|*hostname* } [**-n** *nvalue* |**-system-time**|**-t**|**-q**|**-f**|**-h** *hvalue*|**-l** *lengthvalue*|**-w** *waitvalue*|**-m** *mvalue*|**-tc** *tcvalue*|**-8021p** *8021pvalue*|**-range** *rangevalue*|**-s** *source-ipv6-adress*|**-nexthop** *next-ipv6-address*|**-eth-trunk** *trunk-number*|**-loopback** *loopback-number*|**-vlan** *vlan-id*|**-ge** *interface-number1*|**-10ge** *interface-number2*|**-meth** *meth-number*]	通过 **ping** 命令测试 IPv6 网络的连通性。

说明

在 **ping** 命令执行的过程中，无法对设备进行其他操作，只有等待执行过程结束或者通过“Ctrl＋C”键强制中断执行过程后才能进行其他操作。

10.13 Trace

10.13.1 简介

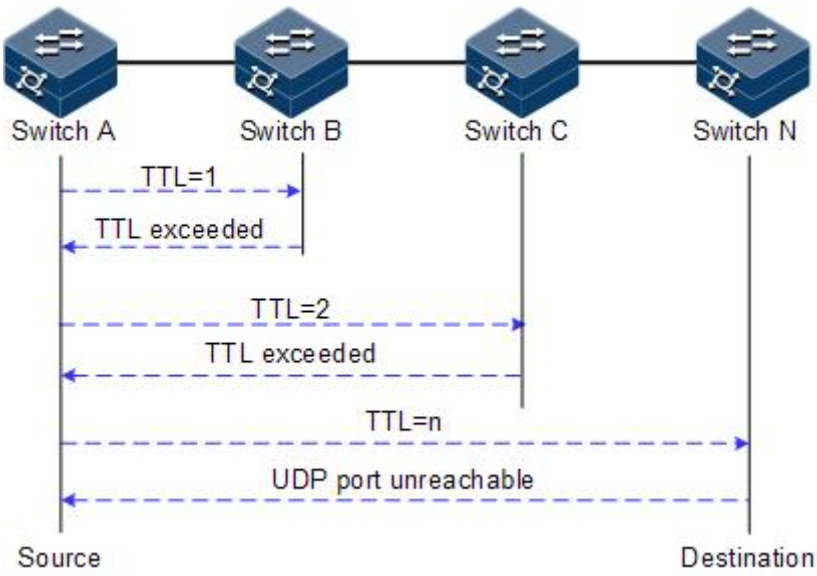
Trace 和 Ping 一样，是网络管理中常用的维护手段。Trace 功能常用于测试报文从发送端到目的端所经过的网络节点，检测网络连接是否可达，并分析网络中的故障点。

Trac 的执行过程如下：

- 首先发送一份 TTL 为 1 的嗅探报文（其中报文的 UDP 端口号是目的端的任何一个应用程序都不可能使用的端口号）。
- 到达第 1 跳时 TTL 减 1，由于 TTL 的值为 0，第 1 跳设备发回一个 ICMP 超时报文，指明此报文不能被发送。
- 发送主机将 TTL 加 1 后重新发送此报文。
- 到达第 2 跳时由于 TTL 的值被减为 0，第 2 跳设备发回一个 ICMP 超时报文，指明此报文不能被发送。

以上步骤循环进行，直到到达目的主机，目的主机并不会送回 ICMP 超时报文，由于目的主机的端口号没有被使用，目的主机会发送端口不可达报文，测试结束。这样，发送主机就能够记录每一个 ICMP TTL 超时报文的源地址，根据得到的回应报文分析出到达目的地所经历的路径。Trace 功能实现原理如图 10-15 所示。

图 10-15 Trace 功能实现原理组网示意图



10.13.2 配置 IPv4 Trace 功能

请在设备上进行以下操作。

步骤	配置	说明
1	JX#**trace** *ip-address* [**-n** *number*|**-r**|**-q**|**-f**|**-fh** *first-ttl-value*|**-h** *max-ttl-value*|**-l** *length-value*|**-w** *wait-for-each-value*|**-tos** *tosvalue*|**-m** *wait-for-send-value*|**-dscp** *dscpvalue*|**-8021p** *8021p-value*|**-range** *range-value*|**-s** *source-ip-address*|**-nexthop** *next-ip-address*|**-eth-trunk** *trunk-number*|**-loopback** *loopback-number*|**-vlan** *vlan-id*|**-ge** *interface-number1*|**-10ge** *interface-number2*|**-meth** *meth-number*]	通过 **trace** 命令测试 IPv4 网络的连通性并查看报文经过的网络节点。

10.13.3 配置 IPv6 Trace 功能

请在设备上进行以下操作。

步骤	配置	说明
1	JX#**trace-ipv6** *ipv6-address* [**-n** *number*|**-r**|**-q**|**-f**|**-fh** *first-ttl-value*|**-h** *max-ttl-value*|**-l** *length-value*|**-w** *wait-for-each-value*|**-m** *wait-for-send-value*|**-tc** *traffic-class-value*|**-8021p** *8021p-value*|**-range** *pkt-length-value*|**-s** *source-ipv6-address*|**-nexthop** *next-ipv6-address*|**-eth-trunk** *trunk-number*|**-loopback** *loopback-number*|**-vlan** *vlan-id*|**-ge** *interface-number1*|**-10ge** *interface-number2*|**-meth** *meth-number*]	通过 **trace** 命令测试 IPv6 网络的连通性并查看报文经过的网络节点。

10.14 硬件监控

说明

不是所有设备都支持温度告警。请以具体设备支持情况为准。

10.14.1 简介

硬件环境监控主要是对设备的运行环境进行监控，监控的对象主要包括设备的温度和电源。

10.14.2 温度监控

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**temperature monitor** { **disable** | **enable** }	使能或去使能温度监控。
3	JX(config)#**temperature** { **all** | *temperature-index* } **description** *description-string*	设置所有或指定温度监控表项的描述信息。
4	JX(config)#**temperature** { **all** | *temperature-index* } **low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*	设置所有或指定温度监控表项的高低门限值，当温度高于高门限值或低于低门限值时都会产生告警。
5	JX(config)#**temperature** { **all** | *temperature-index* } **snmp-trap** { **disable** | **enable** }	使能或去使能所有温度监控表项或指定温度监控表项发送 TRAP 信息的功能。。

10.14.3 电源监控

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**power monitor** { **disable** | **enable** }	使能或去使能电源信息监控。
3	JX(config)#**power monitor interval** *interval-value*	设置电源信息监控的周期，默认值是 25 秒。
4	JX(config)#**power** { **all** | *power-index* } **description** *description-string*	设置所有电源表项或指定电源表项的描述信息。
5	JX(config)#**power** { **all** | *power-index* } **snmp-trap** { **disable** | **enable** }	使能或去使能所有电源监控表项或指定电源监控表项发送 TRAP 信息的功能。

10.14.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

步骤	配置	说明
1	JX#**show temperature config**	显示对温度监控所作的相关配置信息。
2	JX#**show power config**	显示对电源监控所作的相关配置信息。

10.15 风扇监控

说明

本节仅适用于带风扇款型。

10.15.1 简介

设备支持风扇监控功能，可以对风扇的转速和温度进行监控，当设备监控到风扇的转速和温度出现异常时，会产生告警并发送 Trap 信息。

设备对风扇的监控模式有两种：

- 固定转速等级模式，即强制设定风扇的转速等级；
- 温控模式，即风扇根据温度的变化自动调节转速等级。

在温控模式下，当检测到风扇的温度超出高门限值时，就会将风扇的转速等级提升一档，如果检测到风扇的温度低于低门限值时，就会将风扇的转速等级下调一档。

10.15.2 配置准备

场景

当设备安放于比较炎热的环境时，过高的温度会影响设备的散热性能，此时需要配置风扇监控功能，使设备的风扇能够依据周围的环境温度自动调节，以维护设备的正常运转。

前提

无

10.15.3 配置风扇监控功能

请在需要配置风扇监控功能的设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**fan monitor** { **disable** | **enable** }	使能或去使能风扇监控。
3	JX(config)#**fan monitor interval** *interval-value*	配置风扇监控周期。

步骤	配置	说明
4	JX(config)#**fan** { **all** | *fan-index* } **mode** { **speed-level** | **temperature-control** }	配置所有风扇或指定风扇的模式，speed-level 为固定转速等级模式，temperature-control 为温控模式。
5	JX(config)#**fan** { **all** | *fan-index* } **description** *description-string*	配置所有风扇或指定风扇的描述信息。
6	JX(config)#**fan** { **all** | *fan-index* } **level** *level-value*	配置所有风扇或指定风扇的转速等级。
7	JX(config)#**fan** { **all** | *fan-index* } **snmp-trap** { **disable** | **enable** }	使能或去使能所有风扇或指定风扇的 TRAP 发送功能。

10.15.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show fan**	查看风扇监控的相关信息，当前转速、转速等级等信息。
2	JX#**show fan verbose**	查看风扇的基本信息。
3	JX#**show fan config**	查看风扇监控配置的相关信息。

10.16 设备堆叠

10.16.1 简介

堆叠，是指将两台及以上支持堆叠特性的交换机设备组合在一起，从逻辑上形成一台交换设备。使用这种虚拟化技术可以集合多台设备的硬件资源能力和软件处理能力，实现多台设备的协同工作、统一管理和不间断维护。

堆叠基本概念

- 运行模式

设备支持两种运行模式：

普通模式：该模式下，设备不能与其他设备形成堆叠。

堆叠模式：该模式下，进行堆叠配置后可与其他堆叠设备形成堆叠。

当两种堆叠模式切换时，将会引起设备重启。

- 成员设备角色

堆叠中的每台设备都称为成员设备，每个成员设备根据协商的结果，可能处于不同的角色：

Master：主用设备，负责管理和控制整个堆叠系统。

Slave：处理业务、转发报文的同时作为主用设备的备份设备运行。当主用设备故障时，堆叠系统会自动从备设备中选举一个新的主设备接替原主用设备的工作。

- 成员设备编号

堆叠系统使用成员设备编号来标识和管理成员设备。在进行堆叠配置时，必须保证设备的成员设备编号是唯一的，如果两台设备的成员编号是一样的，则在协商时将会出现问题，导致堆叠系统建立出现问题。

- 成员优先级

成员优先级是成员设备的一个属性，默认情况下，设备的成员优先级是 1。在堆叠协商的过程中，成员优先级的大小将影响成员设备是否能被选举成员堆叠主用设备。如果想让某台设备称为堆叠系统的主用设备，可以将设备的成员优先级设置为一个较大的值。

- 堆叠端口

堆叠端口是一个逻辑端口，专门用于堆叠成员设备之间的连接。每台成员设备可以配置两个堆叠端口，堆叠端口需要和物理端口绑定之后才能生效。

- 堆叠域

堆叠域是一个逻辑概念，一个堆叠系统对应一个堆叠域。只有堆叠域 ID 一致的成员设备之间才能建立堆叠系统，不同堆叠域之间的成员设备即使能够收到对端设备的堆叠报文，也无法建立堆叠系统。

堆叠拓扑

本系列交换机可以支持 2 台设备组成堆叠，堆叠设备之间组成链型或环型拓扑的堆叠系统。

图 10-16 2 台成员设备组成链型拓扑

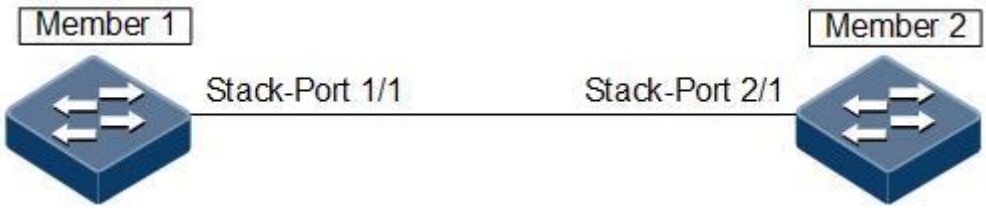
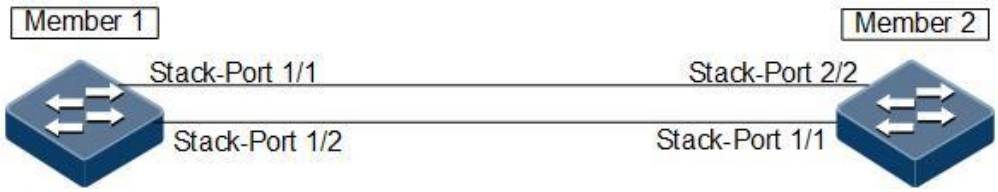


图 10-17 2 台成员设备组成环形型拓扑



注意

成员设备组成环型堆叠拓扑时，相邻两台堆叠成员设备之间的堆叠端口号是不一样的。如图 10-16 所示，堆叠成员设备 1 的堆叠端口 1/1 和堆叠成员设备 2 的堆叠端口的 2/2 相连。如果出现两台相连设备之间相同堆叠端口号一样，在主备切换时将会导致堆叠系统出现同步失败。

堆叠角色选举

当堆叠系统出现如下情况时都将进行角色选举：

- 堆叠系统建立。
- 堆叠系统分裂，即堆叠链路断开。
- 两个独立运行的堆叠系统合并。

角色选举时将按照如下优先级选举主备设备：

- 当前的主设备优先，如果是两个独立堆叠系统合并，此时将在两个对立堆叠系统的主用设备中选举出新的主用设备。
- 成员设备配置了强制为主的设备。
- 成员设备优先级大的设备。
- 系统运行时间长的设备，如果设备启动时间间隔超过 1 分钟，则运行时间长的设备优先。
- 成员设备的 mac 地址，mac 地址小的设备优先。

通过如上规则选举出来的最优设备即为主用设备，其他设备为从设备。

10.16.2 堆叠缺省配置

堆叠功能相关缺省值如下：

功能	缺省值
堆叠功能	禁用
堆叠成员优先级	1
堆叠成员编号	1
堆叠成员所属域 ID	1
堆叠成员发生堆叠协议报文时间间隔	3（单位秒）

10.16.3 配置堆叠

请在设备上进行以下配置：

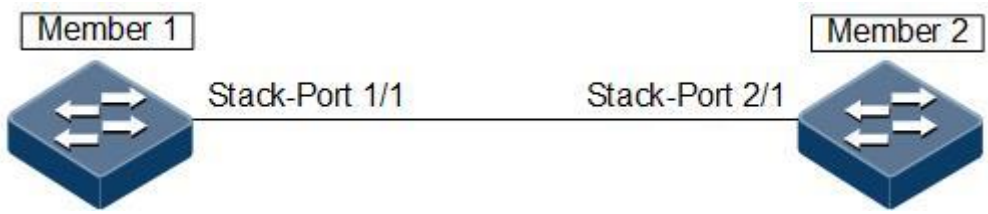
步骤	配置	说明
1	JX(config)#**interface stack-port** *number*	创建堆叠端口。
2	JX(config-stack-port-*number*)#**add interface** *interface-type interface-number*	将物理端口添加值堆叠端口。
3	JX(config)#**hvs hello-interval** { *time* | **default** }	配置堆叠协议发生报文的时间间隔，单位秒，取值范围为 1～10，默认值为 3。
4	JX(config)#**hvs master**	配置堆叠成员在堆叠协商时强制为主用设备。
5	JX(config)#**hvs member-id** *id*	配置堆叠设备的成员编号。
6	JX(config)#**hvs priority** *value*	配置堆叠成员设备的优先级。
7	JX(config)#**hvs switch-master member** { **myself** | *id* }	配置堆叠系统进行主备切换。
8	JX(config)#**hvs mode** { **normal** | **stack** }	配置堆叠成员设备进行模式切换，模式切换后设备将自动重启。
9	JX(config)#**show hvs member**	查看当前堆叠系统中成员以及主备角色
10	JX(config)#**show hvs topo**	查看整个堆叠系统中的拓扑信息
11	JX(config)#**show hvs interface**	查看本设备堆叠端口的信息
12	JX(config)#**show hvs config**	查看本设备堆叠相关配置

10.16.4 配置举例

组网需求

如下图的拓扑结构，如果 2 台设备需要组建链型拓扑结构的堆叠系统，需要进行如下配置。

图 10-18 2 台堆叠拓扑图



配置步骤

步骤 1 设备 1 的配置：

```
JX(config)#interface stack-port 1
JX(config-stack-port-1)#add interface ge 1/0/1
JX(config-stack-port-1)#add interface ge 1/0/2
JX(config-stack-port-2)#quit
JX(config)#hvs member-id 1
JX(config)#hvs mode stack
```

步骤 2 设备 2 的配置：

```
JX(config)#interface stack-port 1
JX(config-stack-port-1)#add interface ge 1/0/1
JX(config-stack-port-1)#add interface ge 1/0/2
JX(config-stack-port-1)#quit
JX(config)#hvs member-id 2
JX(config)#hvs mode stack
```

步骤 3 待到 2 台设备重启完成之后，它们之间就会开始协商，然后可以通过命令查看堆叠是否建立完成。

检查配置

此时在设备 2 上通过 **show hvs member** 的命令的结果如下：

```
JX(config)#show hvs member
  NOTE: '*' indicates the device is myself

  SysId Role/ConfRole  State/Pri     Mac           Uptime
-------------------------------------------------------------------------
  1    master/no     done/1        f0f1:f2f3:0101  12d:18h:16m:06s
* 2    slave/no      done/1        f0f1:f2f3:0201  12d:18h:16m:04s
-------------------------------------------------------------------------
```

通过 show hvs topo 的命令的结果如下：

```
JX(config)#show hvs topo
 Interface: stack-port-2/1,  State: up,  MAC: f0:f1:f2:f3:02:01

 Hop   SysId    MAC
---------------------------------------------
 0     2        f0:f1:f2:f3:02:01
 1     1        f0:f1:f2:f3:01:01
---------------------------------------------
```

10.17 MAD

10.17.1 简介

当堆叠系统中成员设备之间链路端口，可能会导致堆叠系统分裂称为多个新的堆叠系统，这些新的堆叠系统有相同的 IP 地址等三层配置，会引起地址冲突，导致网络故障。MAD(Multi-Active Detection，多主冲突检测)协议用来进行堆叠分裂检测、冲突处理和故障恢复，以提高系统的可用性。

MAD 协议检测冲突主要有几种工作模式。

- 直连模式

直连模式下，需要在要进行多主冲突检测的堆叠成员设备之间分配一个额外的物理端口，用于收发 MAD 协议报文，可如图 10-18 建立拓扑。

- 代理模式

代理模式下，需要另外一个设备启用 MAD 协议，然后该设备与堆叠的各个成员设备之间建立跨设备聚合链路，然后在该聚合口上使能 MAD 协议，可如图 10-19 建立拓扑。

带外口检测模式

该模式下，只需要在带外口使能 MAD 协议，并且将所有堆叠成员设备的带外口连接到同一交换机，且保证所有带外口之间能正常通信即可。

图 10-19 MAD 直连模式

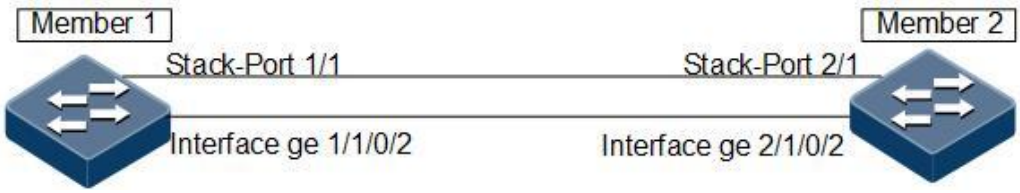
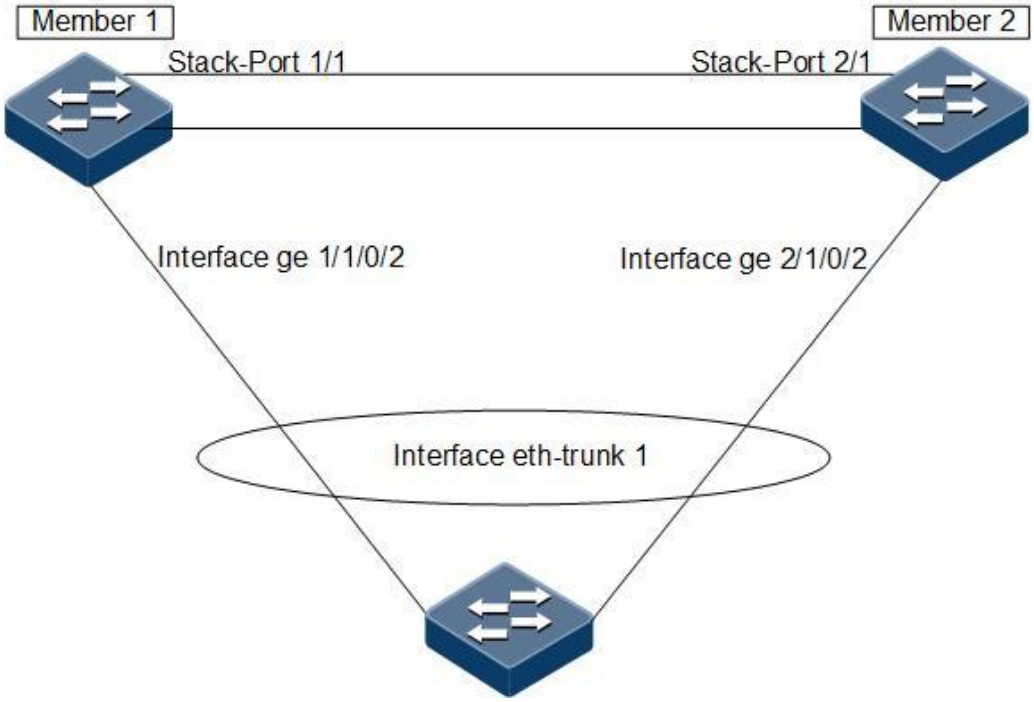


图 10-20 MAD 代理模式



10.17.2 配置准备

场景

- 备用管理 IP 地址

MAD 协议除了可以配置端口的工作模式外，可以为每个堆叠成员配置一个备份 IP 地址，该 IP 在 MAD 协议检测到多主时，自动将设备的带外口设置为该 IP 地址。

- 保留端口

MAD 协议在检测到多主时，进行比较之后，如果发现自己不是优选设备，则会将设备自己的端口进行 shutdown 操作。如果用户不想某些端口在 MAD 检测到多主时被 shutdown，可以进行保留端口的配置。

前提

无

10.17.3 配置 MAD

请在设备上进行如下配置：

步骤	配置	说明
1	JX(config)#**multi-active-detect backup ip address** *ip-address* **member** { **all** | *member-id*}	为指定的堆叠成员设备设置备份管理 IPv4 地址。
2	JX(config)#**multi-active-detect backup ipv6 address** *ipv6-address* **member** { **all** | *member-id*}	为指定的堆叠成员设备设置备份管理 IPv6 地址。
3	JX(config)#**interface GE 1/0/0/*** JX(config-ge-1/1/0/*)#**multi-active-detect mode direct**	配置该端口下 MAD 协议的工作模式。
4	JX(config)#**interface eth-trunk 1** JX(config-eth-trunk-1)#**multi-active-detect mode relay**	配置该聚合组端口下 MAD 协议的工作模式。
5	JX(config)#**interface meth 0/0/0** JX(config-meth-0/0/0)#**multi-active-detect** { **disable** | **enable** } JX(config)#**interface GE 1/0/0/*** JX(config-ge-1/1/0/*)#**multi-active-detect** { **disable** | **enable** }	在端口下使能或去使能 MAD 协议。
6	JX(config-meth-0/0/0)#**multi-active-exclude** { **disable** | **enable** }	在端口下使能 MAD 保留端口功能。
7	JX(config)#**show multi-active-detect config**	查看当前设备上的 MAD 相关配置。
8	JX(config)#**show multi-active-detect information**	查看你当前设备上 MAD 协议相关状态。

10.17.4 配置举例

组网需求

如图 10-8，首先需要进行堆叠向配置，让两台设备建立堆叠系统，然后在配置 MAD。

配置步骤

步骤 1 设备 1 的配置：

```
JX(config)#interface stack-port 1
JX(config-stack-port-1)#add interface ge 1/0/1
JX(config-stack-port-1)#quit
JX(config)#hvs member-id 1
JX(config)#hvs mode stack
```

步骤 2 设备 2 的配置：

```
JX(config)#interface stack-port 1
JX(config-stack-port-1)#add interface ge 1/0/1
JX(config-stack-port-1)#quit
JX(config)#hvs member-id 2
JX(config)#hvs mode stack
```

步骤 3 待到两台设备建立堆叠系统后，开始进行 MAD 协议相关配置。

```
JX(config)#interface GE 1/0/0/2
JX(config-ge-1/1/0/2))#stp disable
JX(config-ge-1/1/0/2))#multi-active-detect mode direct
JX(config-ge-1/1/0/2)#quit
JX(config)#interface ge 2/1/0/2
JX(config-ge-1/1/0/2))#stp disable
JX(config-ge-2/1/0/2))#multi-active-detect mode direct
```

检查配置

此时将堆叠端口端口，然后通过命令 **show multi-active-detect information** 查看 MAD 协议状态。

设备 1 状态：

```
JX(config)#show multi-active-detect information
  Current status : normal
  Direct detect information:
    ge-1/1/0/2     up
  Excluded ports(configurable):
    ge-1/1/0/5
  Excluded ports(can not be configured):
    ge-1/1/0/1
```

设备 2 状态：

```
JX(config)#show multi-active-detect information
  Current status : conflict
  Direct detect information:
    ge-2/1/0/2     up
  Excluded ports(configurable):
    ge-2/1/0/5
  Excluded ports(can not be configured):
    ge-2/1/0/1
```

10.18 NQA

10.18.1 简介

网络质量分析 NQA（Network Quality Analysis）是一种实时的网络性能探测和统计技术，可以对响应时间、网络抖动、丢包率等网络信息进行统计。NQA 能够实时监视网络 QoS，在网络发生故障时进行有效的故障诊断和定位。

10.18.2 配置准备

场景

为了使网络服务质量可见，使用户能够自行检查网络服务质量是否达到要求。需要在网络中部署探针设备对网络服务质量进行监控。

当设备提供 NQA 时，就不用部署专门的探针设备，可以有效的节约成本。NQA 可以实现对网络运行状况的准确测试，输出统计信息。

NQA 监测网络上运行的多种协议的性能，使用户能够实时采集到各种网络运行指标，例如：HTTP 的总时延、TCP 连接时延、DNS 解析时延、文件传输速率、FTP 连接时延、DNS 解析错误率等。

前提

无

10.18.3 NQA 的缺省配置

设备上 NQA 功能的缺省配置如下。

功能	缺省值
NQA 功能	禁用

10.18.4 配置 ICMP-echo 测试

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **type icmp-echo**	配置测试实例,类型为 icmp-echo
3	JX(nqa-admin-test-icmp-echo)#**destination ip** *ip-address*	配置目的 ip 地址
4	JX(nqa-admin-test-icmp-echo)#**frequency** *freq-ms*	配置测试频率，单位：毫秒
5	JX(nqa-admin-test-icmp-echo)#**probe count** *count*	配置每次测试探测的次数
6	JX(nqa-admin-test-icmp-echo)#**probe timeout** *timeout-time-ms*	配置每次探测等待的时间，单位：毫秒

7	JX(config)#**nqa schedule** *admin-name operate-tag* **start-time now life-time forever**	配置检测调度策略为立即开始，一直循环 注：该配置与绑定 timerange 策略二选一即可
8	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	配置检测调度策略绑定 timerange 注：该策略与立即开始策略二选一即可

10.18.5 配置 UDP-echo 测试

请在服务端设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**nqa server enable**	配置 nqa 服务端使能
3	JX(config)#**nqa server udp-connect** *ip-address udp-port*	配置 udp 服务端

请在客户端设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **type udp-echo**	配置测试实例,类型为 udp-echo
3	JX(nqa-admin-test-udp-echo)#**destination ip** *ip-address*	配置目的 ip 地址
4	JX(nqa-admin-test-udp-echo)#**destination port** *udp-port*	配置目的 udp 端口号
5	JX(nqa-admin-test-udp-echo)#**frequency** *freq-ms*	配置测试频率，单位：毫秒
6	JX(nqa-admin-test-udp-echo)#**probe count** *count*	配置每次测试探测的次数
7	JX(nqa-admin-test-udp-echo)#**probe timeout** *timeout-time-ms*	配置每次探测等待的时间，单位：毫秒
8	JX(config)#**nqa schedule** *admin-name operate-tag* **start-time now life-time forever**	配置检测调度策略为立即开始，一直循环 注：该配置与绑定 timerange 策略二选一即可
9	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	配置检测调度策略绑定 timerange 注：该策略与立即开始策略二选一即可

10.18.6 配置 TCP 测试

请在服务端设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**nqa server enable**	配置 nqa 服务端使能
3	JX(config)#**nqa server tcp-connect** *ip-address tcp-port*	配置 tcp 服务端

请在客户端设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **type tcp**	配置测试实例,类型为 tcp
3	JX(nqa-admin-test-tcp)#**destination ip** *ip-address*	配置目的 ip 地址
4	JX(nqa-admin-test-tcp)#**destination port** *tcp-port*	配置目的 tcp 端口号
5	JX(nqa-admin-test-tcp)#**frequency** *freq-ms*	配置测试频率，单位：毫秒
6	JX(nqa-admin-test-tcp)#**probe count** *count*	配置每次测试探测的次数
7	JX(nqa-admin-test-tcp)#**probe timeout** *timeout-time-ms*	配置每次探测等待的时间，单位：毫秒
8	JX(config)#**nqa schedule** *admin-name operate-tag* **start-time now life-time forever**	配置检测调度策略为立即开始，一直循环 注：该配置与绑定 timerange 策略二选一即可
9	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	配置检测调度策略绑定 timerange 注：该策略与立即开始策略二选一即可

10.18.7 配置 DNS 测试

请在设备上进行以下配置。

步骤	配置	说明

1	JX#**configure**	进入全局配置模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **type dns**	配置测试实例,类型为 dns
3	JX(nqa-admin-test-dns)#**destination ip** *ip-address*	配置 DNS 服务器地址
4	JX(nqa-admin-test-dns)#**resolve-target** *domain-name*	配置需要解析的域名
5	JX(nqa-admin-test-tcp)#**frequency** *freq-ms*	配置测试频率，单位：毫秒
6	JX(nqa-admin-test-tcp)#**probe count** *count*	配置每次测试探测的次数
7	JX(nqa-admin-test-tcp)#**probe timeout** *timeout-time-ms*	配置每次探测等待的时间，单位：毫秒
8	JX(config)#**nqa schedule** *admin-name operate-tag* **start-time now life-time forever**	配置检测调度策略为立即开始，一直循环 注：该配置与绑定 timerange 策略二选一即可
9	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	配置检测调度策略绑定 timerange 注：该策略与立即开始策略二选一即可

10.18.8 配置 HTTP 测试

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **type http**	配置测试实例,类型为 http
3	JX(nqa-admin-test-http)#**destination ip** *ip-address*	配置 HTTP 服务器地址
4	JX(nqa-admin-test-http)#**url** *url-path*	配置探测的 URL
5	JX(nqa-admin-test-http)#**frequency** *freq-ms*	配置测试频率，单位：毫秒
6	JX(nqa-admin-test-http)#**probe count** *count*	配置每次测试探测的次数
7	JX(nqa-admin-test-http)#**probe timeout** *timeout-time-ms*	配置每次探测等待的时间，单位：毫秒
8	JX(config)#**nqa schedule** *admin-name operate-tag* **start-time now life-time forever**	配置检测调度策略为立即开始，一直循环 注：该配置与绑定 timerange 策略二选一即可

9	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	配置检测调度策略绑定 timerange 注：该策略与立即开始策略二选一即可

10.18.9 配置 FTP 测试

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **type ftp**	配置测试实例,类型为 ftp
3	JX(nqa-admin-test-ftp)#**destination ip** *ip-address*	配置 FTP 服务器地址
4	JX(nqa-admin-test-ftp)#**username** *ftp-username*	配置 FTP 用户名
5	JX(nqa-admin-test-ftp)#**password** *ftp-password*	配置 FTP 用户密码
6	JX(nqa-admin-test-ftp)#**filename** *ftp-filename*	配置用于探测的文件名
7	JX(nqa-admin-test-ftp)#**operation**（**get|put**）	（可选）配置 ftp 操作，默认：get
5	JX(nqa-admin-test-ftp)#**frequency** *freq-ms*	配置测试频率，单位：毫秒
6	JX(nqa-admin-test-ftp)#**probe count** *count*	配置每次测试探测的次数
7	JX(nqa-admin-test-ftp)#**probe timeout** *timeout-time-ms*	配置每次探测等待的时间，单位：毫秒
8	JX(config)#**nqa schedule** *admin-name operate-tag* **start-time now life-time forever**	配置检测调度策略为立即开始，一直循环 注：该配置与绑定 timerange 策略二选一即可
9	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	配置检测调度策略绑定 timerange 注：该策略与立即开始策略二选一即可

10.18.10 配置 SNMP 测试

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

2	JX(config)#**nqa test-instance** *admin-name operate-tag* **type snmp**	配置测试实例,类型为 snmp
3	JX(nqa-admin-test-snmp)#**destination ip** *ip-address*	配置 SNMP 服务器地址
4	JX(nqa-admin-test-snmp)#**frequency** *freq-ms*	配置测试频率，单位：毫秒
5	JX(nqa-admin-test-snmp)#**probe count** *count*	配置每次测试探测的次数
6	JX(nqa-admin-test-snmp)#**probe timeout** *timeout-time-ms*	配置每次探测等待的时间，单位：毫秒
7	JX(config)#**nqa schedule** *admin-name operate-tag* **start-time now life-time forever**	配置检测调度策略为立即开始，一直循环 注：该配置与绑定 timerange 策略二选一即可
8	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	配置检测调度策略绑定 timerange 注：该策略与立即开始策略二选一即可

10.18.11 配置测试历史记录功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **{ type (icmp-echo|udp-echo|tcp|dns|http|ftp|snmp) }**	进入任意 nqa 测试实例
3	JX(nqa-admin-test-icmp-echo)#**history-record enable**	使能历史记录功能
	JX(nqa-admin-test-icmp-echo)#**history-record keep-time** *time-minutes*	（可选）配置历史记录保存时间，单位：分钟

10.18.12 配置测试统计功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局模式。

2	JX(config)#**nqa test-instance** *admin-name operate-tag* **{ type (icmp-echo|udp-echo|tcp|dns|http|ftp|snmp) }**	进入任意 nqa 测试实例
3	JX(nqa-admin-test-icmp-echo)#**statistics enable**	使能测试统计功能
4	JX(nqa-admin-test-icmp-echo)#**statistics interval** *interval-minutes*	（可选）配置统计周期

10.18.13 配置测试告警功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局模式。
2	JX(config)#**nqa test-instance** *admin-name operate-tag* **{ type (icmp-echo|udp-echo|tcp|dns|http|ftp|snmp) }**	进入任意 nqa 测试实例
3	SwitchA(nqa-admin-test-icmp-echo)#**reaction trap probe-failure** *fail-count*	每次探测连续发生 n 次失败时，发送 trap
4	SwitchA(nqa-admin-test-icmp-echo)#**reaction trap test-failure** *fail-count*	每次探测累积发生 n 次失败时，发送 trap
5	SwitchA(nqa-admin-test-icmp-echo)#**reaction trap test-complete**	每次探测完成，发送 trap

10.18.14 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show nqa config**	查看 nqa 配置信息。

10.18.15 维护

用户可以通过以下命令维护 NQA 特性。

命令	描述
JX#**show nqa agent**	查看 nqa 客户端信息
JX#**show nqa server**	查看 nqa 服务端信息

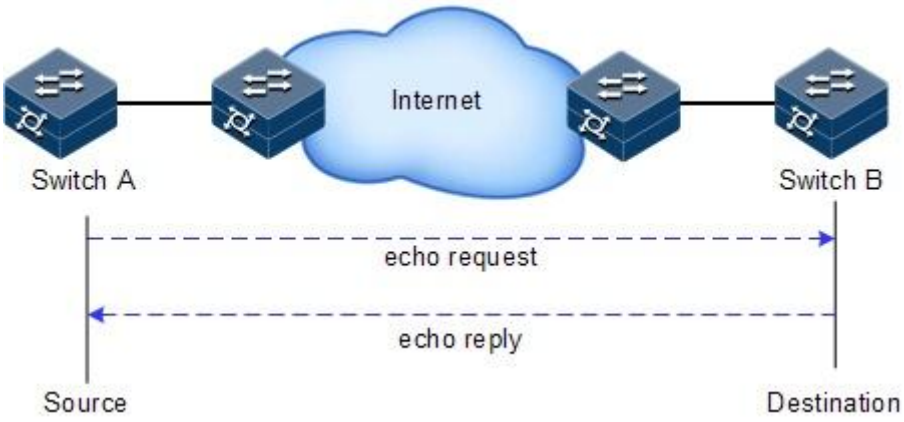
命令	描述
JX#**show nqa result** *admin-name operate-tag*	查看 nqa 客户端测试结果
JX#**show nqa history** *admin-name operate-tag*	查看 nqa 客户端测试结果历史
JX#**show nqa statistics** *admin-name operate-tag*	查看 nqa 客户端测试结果统计

10.18.16 配置 ICMP-echo 测试功能示例

组网需求

如图 10-9 所示，在 Switch A 使能 NQA icmp-echo 探测，探测 SwitchA 与 SwitchB 之间的 IP 层连通性。

图 10-21 配置 ICMP-echo 测试功能组网示意图



配置步骤

步骤 1 配置 IP 层互通。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#vlan 10
SwitchA(config-vlan-10)#quit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port hybrid vlan 10 tagged
SwitchA(config-ge-1/0/1)#quit
SwitchA(config)#interface vlan 10
SwitchA(config-vlanif-10)#ip address 10.1.1.1/24
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#config
```

```
SwitchB(config)#vlan 10
SwitchB(config-vlan-10)#quit
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port hybrid vlan 10 tagged
SwitchB(config-ge-1/0/1)#quit
SwitchB(config)#interface vlan 10
SwitchB(config-vlanif-10)#ip address 10.1.1.2/24
```

步骤 2 配置 NQA 的 icmp-echo 探测实例。

配置 Switch A。

```
SwitchA(config)#nqa test-instance admin test type icmp-echo
SwitchA(nqa-admin-test-icmp-echo)#destination ip 10.1.1.2
SwitchA(nqa-admin-test-icmp-echo)#frequency 10000
SwitchA(nqa-admin-test-icmp-echo)#probe count 3
SwitchA(nqa-admin-test-icmp-echo)#history-record enable
SwitchA(nqa-admin-test-icmp-echo)#reaction trap probe-failure 3
SwitchA(config)#nqa schedule admin test start-time now life-time forever
```

检查结果

通过 **show nqa config** 命令查看本地配置是否正确。

```
SwitchA(config)#show nqa config
!
nqa test-instance admin test type icmp-echo
 frequency 10000
 history-record enable
 statistics enable
 reaction trap probe-failure 3
 probe count 3
 destination ip 10.1.1.2
nqa schedule admin test start-time now life-time forever
……
```

通过 **show nqa history admin test** 命令查看测试结果历史。

```
SwitchA(config)#show nqa history admin test
 Index    Response          Status            Time
--------------------------------------------------------------------------------
1        9                successed         2023-11-10 17:05:05
2        8                successed         2023-11-10 17:05:05
3        11               successed         2023-11-10 17:05:05
4        9                successed         2023-11-10 17:05:16
5        7                successed         2023-11-10 17:05:16
6        12               successed         2023-11-10 17:05:16
7        10               successed         2023-11-10 17:05:26
8        7                successed         2023-11-10 17:05:26
9        11               successed         2023-11-10 17:05:26

--------------------------------------------------------------------------------
```

10.19 POE

10.19.1 简介

以太网供电 PoE（Power over Ethernet）是指通过以太网网络进行供电，也被称为基于局域网的供电系统 PoL（Power over LAN）或有源以太网（Active Ethernet）。

10.19.2 配置准备

场景

随着网络中 IP 电话、网络视频监控以及无线以太网应用的日益广泛，通过以太网本身提供电力支持的要求也越来越迫切。多数情况下，接入点设备需要直流供电，而接入点设备通常安装在距离地面比较高的天花板或室外，附近很难有合适的电源插座，即使有插座，接入点设备需要的交直流转换器也难有位置安置。在很多大型的局域网应用中，管理员同时需要管理多个接入点设备，这些设备需要统一的供电和统一的管理，给供电管理带来极大的不便，以太网供电 PoE 则正好解决了这个问题。

PoE 是一种有线以太网供电技术，是目前本地局域网应用最广泛的一种技术。PoE 允许电功率通过传输数据的线路或空闲线路传输到终端设备。通过 10BASE-T、100BASE-TX、1000BASE-T 以太网网络供电，其可靠供电的距离最长可达到 100 米。通过这种方式，可以有效的解决 IP 电话、无线 AP（Access Point）、便携设备充电器、刷卡机、摄像头、数据采集等终端的集中式电源供电。对于这些终端而言不再需要考虑其室内电源系统布线的问题，在接入网络的同时就可以实现对设备的供电。

前提

无

10.19.3 POE 的缺省配置

设备上 NQA 功能的缺省配置如下。

功能	缺省值
POE 功能	开启
POE 端口工作模式	自动模式

10.19.4 使能 POE 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。

2	JX(config)#**interface** *interface-type interface-number*	进入物理口配置视图 注：进入的物理口需要支持 POE 功能
3	JX(config-ge-1/0/1)#**poe** { **enable** | **disable** }	配置 POE 功能使能/去使能
4	JX(config-ge-1/0/1)#**poe power-management** { **auto** | **manual** | **default** }	配置 POE 工作模式

10.19.5 配置 POE 最大功率

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理口配置视图 注：进入的物理口需要支持 POE 功能
3	JX(config-ge-1/0/1)#**poe max-power** *power-value*	配置 POE 最大功率

10.19.6 配置 POE 上下电管理

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理口配置视图 注：进入的物理口需要支持 POE 功能
3	JX(config-ge-1/0/1)#**poe power-priority** { **critical** | **high** | **low** | **default** }	配置 POE 接口供电优先级 注：部分设备不支持，详细参考设备说明
4	JX(config-ge-1/0/1)#**poe** { **power-on** | **power-off** }	配置 POE 接口手动模式上下电
5	JX(config-ge-1/0/1)#**poe shutdown time-range** *timer-range-list*	配置 POE 接口下电时段
6	JX(config-ge-1/0/1)#**poe inrush** { **af** | **af-high** | **at** | **bt3** | **bt4** | **default** | **pre-at**| **pre-bt3** | **pre-bt4** }	配置 POE 接口供电标准
7	JX(config-ge-1/0/1)#**poe high-inrush** { **enable** | **disable** }	配置 POE 接口允许 PD 设备上电瞬间的高冲击电流

10.19.7 配置 PD 描述

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理口配置视图 注：进入的物理口需要支持 POE 功能
3	JX(config-ge-1/0/1)#**poe description** descr-str	配置 PD 描述

10.19.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show poe config**	查看 poe 配置信息。

10.19.9 维护

用户可以通过以下命令维护 POE 特性。

命令	描述
JX#**show poe information**	查看设备 POE 的支持情况
JX#**show poe interface**	查看 POE 端口的供电情况

10.19.10 配置 POE 示例

组网需求

POE 接口 GE1/0/1，GE1/0.2，GE1/0/3 连接三台 PD 设备

配置步骤

步骤 1 配置工作模式为自动。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#poe power-management auto
```

```
JX(config-ge-1/0/1)#quit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#poe power-management auto
JX(config-ge-1/0/2)#quit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#poe power-management auto
JX(config-ge-1/0/3)#quit
```

步骤 2 配置 POE 接口最大供电功率。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#poe max-power 1500
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#poe max-power 1500
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#poe max-power 1500
```

步骤 3 配置 POE 接口供电优先级。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#poe power-priority critical
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#poe power-priority high
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#poe power-priority high
```

检查结果

通过 **show poe config** 命令查看本地配置是否正确。

```
JX#show poe config
!
interface ge 1/0/1
 poe power-priority critical
 poe max-power 1500
!
interface ge 1/0/2
 poe power-priority high
 poe max-power 1500
!
interface ge 1/0/3
 poe power-priority high
 poe max-power 1500
……
```

通过 **show poe interface** 命令查看测试结果历史。

```
JX#show poe interface

Interface   State   PowerMode      PowerPri   DetectStatus     PowerClass
CurrentPower(mW)  Descr

------------------------------------------------------------------------
-------------------------------------------
```

```
ge-1/0/1    enable  auto          critical   deliveringPower   class4
24000          -

ge-1/0/2    enable  auto          high       searching        --     0
-

ge-1/0/3    enable  auto          high       deliveringPower   class4
24000          -

ge-1/0/4    enable  auto          low        searching        --     0
-

ge-1/0/5    enable  auto          low        searching        --     0
-

ge-1/0/6    enable  auto          low        searching        --     0
-

ge-1/0/7    enable  auto          low        searching        --     0
-

ge-1/0/8    enable  auto          low        searching        --     0
-

--------------------------------------------------------------------------------
----------------------------------------------
```

10.20 U 盘部署

10.20.1 简介

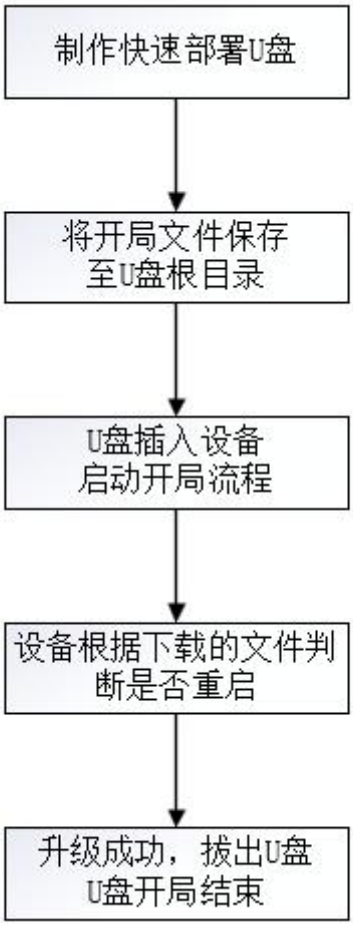
随着网络规模的扩大，网络中需要部署的设备数量越来越多，开局部署也日渐增多。相比传统的通过专业工程师逐台的去给设备部署的模式，U 盘部署功能只需要让专业工程师把所有部署文件存储到 U 盘中即可，具体部署任务可以通过现场非专业人员来进行。这样既简化了开局部署流程，又降低了开局部署成本。

U 盘部署开局时，用户预先将部署文件（系统软件、配置文件、odm 文件）存储在 U 盘中，然后将 U 盘插入设备，设备通过从 U 盘下载部署文件来实现对目标软件版本和相关业务的部署。

10.20.2 U 盘部署流程

U 盘快速部署之前，需要先按照说明制作快速部署 U 盘，并将需要加载的部署文件保存至 U 盘根目录。将 U 盘插入设备中，设备会自动完成部署文件的加载。具体流程如下图所示。

图 10-22 U 盘快速部署流程示意图



10.20.3 配置准备

场景

用于实现设备 U 盘部署功能。

前提

无

10.20.4 U 盘部署的缺省配置

设备部署的缺省配置如下。

功能	缺省值
U 盘部署开关	启用

10.20.5 制作快速部署 U 盘

步骤 1 将空白 U 盘插入 Linux 系统或支持 U 盘部署的设备（建议直接使用设备）。

步骤 2 将 U 盘格式化成 fat32 格式，如下图所示。

1. 删除现有分区（设备上 U 盘设备为/dev/sda，Linux 系统根据实际加载盘符操作）

```
/ram # fdisk /dev/sda

The number of cylinders for this disk is set to 59136.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): d
Selected partition 1

Command (m for help): d
No partition is defined yet!

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table
```

2. 创建新分区

```
/ram # fdisk /dev/sda

The number of cylinders for this disk is set to 59136.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): n
Partition type
   p   primary partition (1-4)
   e   extended
p
Partition number (1-4): 1
First sector (32-121110527, default 32):
Using default value 32
Last sector or +size{,K,M,G,T} (32-121110527, default 121110527):
Using default value 121110527

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table
```

3. 格式化分区

```
mkfs.vfat /dev/sda1
```

步骤 3 卸载 U 盘，完成制作

10.21 PATCH 补丁功能

10.21.1 简介

patch 功能允许在不更换系统软件的情况下，通过补丁方式在线修复系统漏洞，解决软件问题。系统最多支持 32 个补丁。

10.21.2 配置准备

场景

系统发现的问题，可以通过补丁方式进行修复，无需重启设备。

前提

已准备好补丁文件。

10.21.3 加载补丁

设备上加载一个补丁的配置如下。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**patch 1 load** *FILENAME*	加载一个 patch 补丁

10.21.4 激活补丁

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**patch 1 active**	激活 patch 1 补丁

10.21.5 去激活补丁

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**patch 1 deactive**	去激活 patch 1 补丁，使其失效

10.21.6 删除补丁

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**patch 1 delete**	删除 patch 1 补丁，使其失效

10.21.7 维护

用户可以通过以下命令维护补丁特性。

命令	描述
JX#**show patch information**	查看设备的补丁情况

10.21.8 PATCH 示例

组网需求

通过打补丁的方式修复系统功能。

设备和 PC 通过 SNMP 接口互联，PC 上开启 TFTP 软件，以便从设备下载补丁文件。

配置步骤

步骤 1 通过 tftp 协议下载补丁文件到设备

```
JX(config)#tftp get 22.1.1.1 libmspaaa_patch.pat localfile
libmspaaa_patch.pat
```

步骤 2 加载补丁。

```
JX(config)#patch 1 load libmspaaa_patch.pat
```

步骤 3 激活补丁

```
JX(config)#patch 1 active
```

检查结果

通过 **show** patch information 命令查看 patch 状态：

```
JX(config)#show patch information
 Patch max number     : 32
 Patch current number  : 1
```

```
Seq  ProcName   State  Type  Valid  EffetiveTime       PatchName
-------------------------------------------------------------------------
1    mspaaa   ACTIVE  REP   YES    2024-03-20 17:08:52  libmspaaa_patch.pat
```

10.22 定时备份配置功能

10.22.1 简介

定时备份配置功能目前是基于自动上传配置绑定 timerange 实现。

10.22.2 配置准备

场景

定时备份设备的当前配置到指定服务器。

前提

设备和 pc 能 ping 通，并把 pc 端 tftp 或者 ftp 服务器打开。

10.22.3 配置 timerange

设备上配置一个 timerange list，并配置相应的规则配置如下。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**time-range list** *id*	创建一个 timerange 列表，进入节点

3	JX(config-timerange-*)#**time-range** *timerange-id* **absolute from** *hour:minute:second year/month/monthday* **to** *hour:minute:second year/month/monthday* JX(config-timerange-*)#**time-range** *timerange-id* **everyhour** *minute:second* **to** *minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyday** *hour:minute:second* **to** *hour:minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyweek** *hour:minute:second* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } **to** { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } JX(config-timerange-*)#**time-range** *timerange-id* **everymonth** *hour:minute:second monthday* **to** *hour:minute:second monthday* JX(config-timerange-*)#**time-range** *timerange-id* **everyweekend** *hour:minute:second* **to** *hour:minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyyear** *hour:minute:second month/monthday* **to** *hour:minute:second month/monthday*	创建时间段，可应用于自动上传。 对时间段（周期时间段）：是指由ryxxx 描述的以一周为间隔的周期时间，同时可以依靠绝对时间段指时间范围有效日期。 对时间段：是指由 absolute 指定的定的时间范围。可以通过绝对时间指定的时间范围来限制相对时间段期时间段）在什么时间范围生效。 果该时间段配置了多个生效时间，效原则为：周期时间段之间取”，周期时间段和绝对时间段之间“与”

10.22.4 配置自动上传

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**auto-upload start**	启动自动上传功能
3	JX(config)#**auto-upload tftp server** {*ipv4-address*|*ipv6-address*} *remotefile* {**config**|**running-config**|**log**} [**interval** *interval-value*| **port** *port-number*|**time-range** *list-number*]*	配置自动上传 tftp 服务器属性并指定上传的文件，绑定的 timerange 列表
4	JX(config)#**auto-upload ftp server** {*ipv4-address*|*ipv6-address*} *username password remotefile* {**config**|**running-config**|**log**} [**interval** *interval-value*| **port** *port-number*|**time-range** *list-number*]*	配置自动上传 ftp 服务器属性并指定上传的文件，绑定的 timerange 列表

10.22.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

命令	描述
JX#show auto-upload server	查看配置的自动上传表项
JX#show auto-upload config	查看自动上传的配置

10.22.6 定时备份配置示例

组网需求

通过 tftp 方式自动备份设备当前配置到 PC。

设备和 PC 通过 SNMP 接口互联，PC 上开启 TFTP 软件。

配置步骤

步骤 1 配置 timerange list 1 并配置规则 1（以每小时定时备份举例）

```
JX(config)#time-range list 1。
JX(config-timerange-1)#time-range 1 everyhour 3:10 to 13:10
```

步骤 2 配置自动上传属性,启动自动上传功能，创建表项（tftp 服务器地址 192.168.62.1,本地文件为运行配置文件，上传到服务器的文件为 config.txt），并绑定 timerange list 1

```
JX(config)#auto-upload start
JX(config)#auto-upload tftp server 192.168.62.1 config.txt running-config
time-range 1
```

步骤 3 配置完成后，每小时 3 分 10 秒设备会定时上传运行配置文件到 PC 端 tftp 服务器一次

检查结果

通过 **show auto-upload server** 命令查看所配置的自动上传属性：

```
JX(config)#show auto-upload server
 Type  Server               Port    Interval(min) Localfile         Vpn
TimerangeId
------------------------------------------------------------------------
--------------------------
 tftp  192.168.62.1          69     10          running-config     n/a
1
------------------------------------------------------------------------
--------------------------
JX(config)#
```

11 附录

本章介绍了本文档中涉及的缩略语和术语。

- 术语
- 缩略语

11.1 术语

B

半双工	Half-duplex	半双工指在同一时间只能在同一个方向进行的双向通信。一方在接受信息，而另一方在发送信息的通信，即为半双工。
保护地线	Protection Ground Wire	连接设备和保护地的线缆，通常为黄绿相间的同轴线缆。
标签	Label	线缆、机箱以及警告标识。

D

单模光纤	Single Mode Fiber	单模光纤指在同一条光纤中只能传输单个模式光信号的光纤。
第一英里以太网	EFM（Ethernet in the First Mile）	遵循 IEEE 802.3ah 协议，是一种链路级以太网 OAM 技术，针对两台直连设备之间的链路，提供链路连通性检测功能、链路故障监控功能、远端故障通知功能等。EFM 主要用于用户接入的网络边缘的以太网链路。
电气和电子工程师协会	IEEE（Institute of Electrical and Electronics Engineers）	一个国际性的电子技术与信息科学工程师的协会，是世界上最大的专业技术组织之一（成员人数）。

动态 ARP 检测	DAI（Dynamic ARP Inspection）	一种能够验证网络中 ARP 地址解析协议数据报的安全特性。通过 DAI，网络管理员能够拦截、记录和丢弃具有无效 MAC 地址/IP 地址绑定的 ARP 数据包，以防止网络中常见的 ARP 欺骗攻击。
动态主机配置协议	DHCP（Dynamic Host Configuration Protocol）	在网络中动态分配 IP 地址的技术。它可以自动地为网络中的所有客户端分配 IP 地址，从而减轻管理员的工作量，实现 IP 地址集中管理。
多模光纤	Multi-mode Fiber	多模光纤指在同一条光纤中能够传输多个模式光的光纤。

F

访问控制列表	ACL（Access Control List）	访问控制列表是由 permit | deny 语句组成的一系列有顺序的规则，设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。
服务质量	QoS（Quality of Service）	一种网络安全机制，是用来解决网络延迟和阻塞问题的一种技术。当网络过载或拥塞时，QoS 能确保重要业务不被延迟或丢弃，同时保证网络高效运行。

G

故障转移	Failover	提供了一种端口联动方案，可以扩展链路备份的范围。该功能通过监控上行链路并对下行链路进行同步设置，使上层设备的故障迅速传达给下层，从而触发主备切换，避免因上行链路故障无法被下层设备感知而出现的流量丢失。
光纤配线架	ODF（Optical Distribution Frame）	光缆和光通信设备之间的配线连接设备。它是光传输系统中一个重要的配套设施，主要用于光缆终端的光纤熔接、光连接器安装、光路的调接、多余尾纤的存储及光缆的保护等。

H

互联网编号分配委员会	IANA（Internet Assigned Numbers Authority）	主要职能是分配和维护在互联网技术标准（或协议）中的唯一编码和数值，如 IP 地址，组播地址等。

J

激光器自动关断	ALS（Automatic Laser Shutdown）	当光接口的光纤被拔出或光发射器的输出功率过大时，光接口自动关断激光器，防止出现维护或运行风险。

简单网络管理协议	SNMP（Simple Network Management Protocol）	由 IETF（Internet Engineering Task Force，互联网工程任务组）为了解决 Internet 中网络设备的管理问题而提出的一套网络管理协议。SNMP 可以使一个网管系统远程管理所有支持 SNMP 的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件告警等。它是目前 TCP/IP 网络中应用最广泛的网络管理协议。
简单网络时间协议	SNTP（Simple Network Time Protocol）	SNTP 主要用于同步网络中的设备时间。

K

开放最短路径优先	OSPF（Open Shortest Path First）	一种内部网关动态路由协议，用于在单一自治系统内决策路由。
快速生成树协议	RSTP（Rapid Spanning Tree Protocol）	RSTP 是为了弥补 STP（Spanning Tree Protocol，生成树协议）收敛速度慢的不足而开发的。RSTP 在 STP 的基础上进行了改进，实现了网络拓扑快速收敛。

L

链路汇聚控制协议	LACP（Link Aggregation Control Protocol）	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。
链路聚合	Link Aggregation	通过将多个物理以太网端口聚合在一起形成一个逻辑上的聚合组，并把同一聚合组内的多条物理链路视为一条逻辑链路。链路聚合可以实现流量在聚合组各成员端口之间负载分担，在有效的提高了设备之间链路可靠性的同时，还在不进行硬件升级的条件下增大了带宽。

M

密码认证协议	PAP（Password Authentication Protocol）	PPP 认证协议中的密码认证协议，是一种 2 次握手协议，在网络上采用明文方式传输用户名和密码。

Q

全双工	Full-duplex	通信链路上双方可以同时发送和接收数据。
QinQ	Stacked VLAN 或 Double VLAN	是 802.1Q 的扩展，IEEE 在 802.1ad 标准中定义。在运营商的骨干网络（公网）中，报文携带两层的 VLAN Tag：公网 VLAN Tag 和私网 VLAN Tag。公网中私网 VLAN Tag 被当作报文数据部分进行传输。可以分为基本 QinQ 和灵活 QinQ 两种类型。

S

生成树协议	STP（Spanning Tree Protocol）	STP 可以在局域网中消除网络环路，并实现数据链路备份功能。在逻辑上阻断环路，防止广播风暴的产生。当未阻断的链路出现故障时，阻断的链路会被重新激活，充当备份线路的功能。

T

挑战握手认证协议	CHAP（Challenge-Handshake Authentication Protocol）	PPP 认证协议中的挑战握手认证协议，是一种 3 次握手验证协议，只在网络上传输用户名，而不传输用户密码。

V

VLAN 映射	VLAN Mapping	主要功能是将以太网业务报文中的私网 VLAN Tag 替换为运营商的 VLAN Tag，使其按照运营商的 VLAN 转发规则进行传输。在报文从运营商网络转发到对端用户私网时，再按照同样的规则将 VLAN Tag 恢复为原有的用户私网 VLAN Tag，使报文正确到达目的地。

W

网络时间协议	NTP（Network Time Protocol）	由 RFC1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。使用 NTP 的目的是快速对网络内所有具有时钟的设备进行时钟同步，从而使设备能够提供基于统一时间的不同应用。同时 NTP 还能保证很高的精度（误差在 10ms 左右）。

X

虚拟局域网	VLAN（Virtual Local Area Network）	是为解决以太网的广播问题和安全性而提出的一种协议。是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现多个互不影响的虚拟工作组的二层隔离技术。

Y

以太网承载 PPP 协议	PPPoE（Point-to-point Protocol over Ethernet）	通过 PPPoE 协议，远端接入设备能够实现对每个接入用户的控制和计费。

以太网环网保护倒换	ERPS（Ethernet Ring Protection Switching）	基于 ITU-T G.8032 标准的 APS（Automatic Protection Switching，自动保护倒换）协议，是一种专门应用于以太网环的链路层协议，正常情况下，它在以太网环中能够防止数据环路引起的广播风暴，当以太网环上链路或设备故障时，能迅速切换到备份链路，保证业务快速恢复。
因特网工程任务组	IETF（Internet Engineering Task Force）	成立于 1985 年底，是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定。
远程用户拨号认证系统	RADIUS（Remote Authentication Dial In User Service）	网络中对用户进行认证和计费的协议。

Z

自动保护倒换	APS（Automatic Protection Switched）	自动保护倒换技术是通过对传输线路变化的实时监视、告警信息的自动分析，能够及时发现故障及隐患，在出现严重故障时，快速将工作通道自动切换到备用通道，在极短的时间内恢复通信，完成对故障的快速反应和恢复机制。
自协商	Auto-Negotiation	自协商指接口根据协商结果自动选择接口速率和双工模式。

11.2 缩略语

A

AAA	Authentication，Authorization and Accounting	认证、授权和计费
ABR	Area Border Router	区域边界路由器
AC	Alternating Current	交流电
ACL	Access Control List	访问控制列表
ANSI	American National Standards Institute	美国国家标准协会
APS	Automatic Protection Switching	自动保护倒换
ARP	Address Resolution Protocol	地址解析协议
AS	Autonomous System	自治系统
ASCII	American Standard Code for Information Interchange	美国信息交换标准码

ASE	Autonomous System External	外部自治系统
ATM	Asynchronous Transfer Mode	异步传输模式
AWG	American Wire Gauge	美国线缆标准

B

BC	Boundary Clock	边界时钟
BDR	Backup Designated Router	备份指定路由器
BITS	Building Integrated Timing Supply System	通信楼综合定时供给系统
BOOTP	Bootstrap Protocol	自举协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
BTS	Base Transceiver Station	基站收发信台

C

CAR	Committed Access Rate	承诺访问速率
CAS	Channel Associated Signaling	随路信令
CBS	Committed Burst Size	承诺突发数据量
CE	Customer Edge	用户网边缘
CHAP	Challenge Handshake Authentication Protocol	挑战握手认证协议
CIDR	Classless Inter-Domain Routing	无类域间路由
CIR	Committed Information Rate	承诺信息速率
CIST	Common Internal Spanning Tree	公共内部生成树
CLI	Command Line Interface	命令行接口
CoS	Class of Service	服务等级
CPU	Central Processing Unit	中央处理器
CRC	Cyclic Redundancy Check	循环冗余校验
CSMA/CD	Carrier Sense Multiple Access/Collision Detection	载波侦听多路访问
CST	Common Spanning Tree	公共生成树

D

DAI	Dynamic ARP Inspection	动态 ARP 检测

DBA	Dynamic Bandwidth Allocation	动态带宽分配
DC	Direct Current	直流电
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DiffServ	Differentiated Service	区分服务
DNS	Domain Name System	域名系统
DS	Differentiated Services	差分服务
DSL	Digital Subscriber Line	数字用户线

E

EAP	Extensible Authentication Protocol	PPP 扩展认证协议
EAPoL	EAP over LAN	基于局域网的 EAP
EFM	Ethernet in the First Mile	第一英里以太网
EMC	Electro Magnetic Compatibility	电磁兼容
EMI	Electro Magnetic Interference	电磁干扰
EMS	Electro Magnetic Susceptibility	电磁敏感性
ERPS	Ethernet Ring Protection Switching	以太网环网保护倒换
ESD	Electro Static Discharge	静电释放
EVC	Ethernet Virtual Connection	以太网虚连接

F

FCS	Frame Check Sequence	帧校验序列
FE	Fast Ethernet	快速以太网
FIFO	First Input First Output	先入先出
FTP	File Transfer Protocol	文件传输协议

G

GARP	Generic Attribute Registration Protocol	通用属性注册协议
GE	Gigabit Ethernet	千兆以太网
GMRP	GARP Multicast Registration Protocol	基于 GARP 的组播注册协议
GPS	Global Positioning System	全球定位系统
GVRP	Generic VLAN Registration Protocol	通用 VLAN 注册协议

H

HDLC	High-level Data Link Control	高级数据链路控制
HTTP	Hyper Text Transfer Protocol	超文本传输协议

I

IANA	Internet Assigned Numbers Authority	互联网编号分配委员会
ICMP	Internet Control Message Protocol	Internet 控制报文协议
IE	Internet Explorer	IE 浏览器
IEC	International Electro technical Commission	国际电子技术委员会
IEEE	Institute of Electrical and Electronics Engineers	电气和电子工程师协会
IETF	Internet Engineering Task Force	因特网工程任务组
IGMP	Internet Group Management Protocol	因特网组管理协议
IP	Internet Protocol	网络互联协议
IS-IS	Intermediate System to Intermediate System Routing Protocol	中间系统到中间系统的路由选择协议
ISP	Internet Service Provider	Internet 服务提供商
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector	国际电信联盟远程通信标准化组织

L

LACP	Link Aggregation Control Protocol	链路汇聚控制协议
LACPDU	Link Aggregation Control Protocol Data Unit	链路聚合控制协议数据单元
LAN	Local Area Network	局域网
LCAS	Link Capacity Adjustment Scheme	链路容量调整机制
LLDP	Link Layer Discovery Protocol	链路层发现协议
LLDPDU	Link Layer Discovery Protocol Data Unit	链路层发现协议数据单元

M

MAC	Medium Access Control	媒体访问控制
MDI	Medium Dependent Interface	介质相关接口

MDI-X	Medium Dependent Interface cross-over	介质相关交叉接口
MIB	Management Information Base	管理信息库
MSTI	Multiple Spanning Tree Instance	多生成树实例
MSTP	Multiple Spanning Tree Protocol	多生成树协议
MTBF	Mean Time Between Failure	平均无故障工作时间
MTU	Maximum Transmission Unit	最大传输单元
MVR	Multicast VLAN Registration	组播 VLAN 注册

N

NMS	Network Management System	网络管理系统
NNM	Network Node Management	网络节点管理
NTP	Network Time Protocol	网络时间协议
NView NNM	NView Network Node Management	NView 网络节点管理系统

O

OAM	Operation，Administration and Management	操作、管理和维护
OC	Ordinary Clock	普通时钟
ODF	Optical Distribution Frame	光纤配线架
OID	Object Identifiers	对象标识符
Option 82	DHCP Relay Agent Information Option	DHCP 中继代理信息选项
OSPF	Open Shortest Path First	开放最短路径优先

P

P2MP	Point to Multipoint	点到多点
P2P	Point-to-Point	点到点
PADI	PPPoE Active Discovery Initiation	PPPoE 活动发现发起报文
PADO	PPPoE Active Discovery Offer	PPPoE 活动发现提供报文
PADS	PPPoE Active Discovery Session-confirmation	PPPoE 活动发现会话确认报文
PAP	Password Authentication Protocol	密码认证协议
PDU	Protocol Data Unit	协议数据单元

PE	Provider Edge	运营商边缘
PIM-DM	Protocol Independent Multicast-Dense Mode	密集模式独立组播协议
PIM-SM	Protocol Independent Multicast-Sparse Mode	稀疏模式独立组播协议
Ping	Packet Internet Grope	因特网包探索器
PPP	Point to Point Protocol	点对点协议
PPPoE	PPP over Ethernet	以太网承载 PPP 协议
PTP	Precision Time Protocol	精确时钟同步协议

Q

QoS	Quality of Service	服务质量

R

RADIUS	Remote Authentication Dial In User Service	远程用户拨号认证系统
RCMP	JX Cluster Management Protocol	甲信集群管理协议
RED	Random Early Detection	随机早期检测
RH	Relative Humidity	相对湿度
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Network Monitoring	远端网络监控
ROS	JX Operating System	甲信操作系统
RPL	Ring Protection Link	环保护链路
RRPS	JX Ring Protection Switching	甲信环保护倒换
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
RSVP	Resource Reservation Protocol	资源预留协议

S

SCADA	Supervisory Control And Data Acquisition	数据采集与监视控制系统
SF	Signal Fail	信号失效
SFP	Small Form-factor Pluggable	小封装可插拔
SFTP	Secure File Transfer Protocol	安全文件传输协议
SLA	Service Level Agreement	服务等级规约

SNMP	Simple Network Management Protocol	简单网络管理协议
SNTP	Simple Network Time Protocol	简单网络时间协议
SP	Strict-Priority	严格优先级调度
SPF	Shortest Path First	最短路径优先
SSHv2	Secure Shell v2	安全外壳协议版本 2
STP	Spanning Tree Protocol	生成树协议

T

TACACS+	Terminal Access Controller Access Control System	终端访问控制器访问控制系统
TC	Transparent Clock	透传时钟
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	普通文件传输协议
TLV	Type Length Value	类型、长度和取值
ToS	Type of Service	服务类型
TPID	Tag Protocol Identifier	标签协议标识
TTL	Time To Live	生存时间

U

UDP	User Datagram Protocol	用户数据包协议
UNI	User Network Interface	用户侧接口
USM	User-Based Security Model	基于用户的安全模型

V

VLAN	Virtual Local Area Network	虚拟局域网
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

W

WAN	Wide Area Network	广域网
WRR	Weight Round Robin	加权循环调度