HUAWEI

Quidway S5000 系列以太网交换机
操作手册

VRP3.10

Quidway S5000 系列以太网交换机

操作手册

资料版本： T1-081687-20040731-C-1.02
产品版本： VRP3.10
BOM 编码： 31161087

华为技术有限公司为客户提供全方位的技术支持。

通过华为技术有限公司代理商购买产品的用户，请直接与销售代理商联系。

直接向华为技术有限公司购买产品的用户，可与就近的华为办事处或用户服务中心联系，也可直接与公司总部联系。

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址：http://www.huawei.com

声明



®、HUAWEI®、华为®、C&C08®、EAST8000®、HONET®、®、视点®、ViewPoint®、INtess®、ETS®、DMC®、TELLIN®、InfoLink®、Netkey®、Quidway®、SYNLOCK®、Radium®、雷霆®、M900/M1800®、TELESIGHT®、Quidview®、Musa®、视点通®、Airbridge®、Tellwin®、Inmedia®、VRP®、DOPRA®、iTELLIN®、HUAWEI OptiX®、C&C08 iNET®、NETENGINE™、OptiX™、iSite™、U-SYS™、iMUSE™、OpenEye™、Lansway™、SmartAX™、边际网™、infoX™、TopEng™均为华为技术有限公司的商标。

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

版本说明

本手册对应产品版本为：VRP3.10。

相关手册

Quidway S5000 系列以太网交换机主要手册及用途如下：

手册名称	用途
《Quidway S5000 系列以太网交换机 安装手册》	介绍了 S5000 系列以太网交换机的安装过程、交换机的启动、软硬件维护与监控等内容。
《Quidway S5000 系列以太网交换机 操作手册》	介绍了入门、端口、VLAN、组播协议、QoS/ACL、集中管理、STP、安全、网络协议、系统管理、组网配置实例等模块的内容。
《Quidway S5000 系列以太网交换机 命令手册》	包括入门、端口、VLAN、组播协议、QoS/ACL、集中管理、STP、安全、网络协议、系统管理等模块的命令解释。

本书简介

《Quidway S5000 系列以太网交换机 操作手册》章节安排如下：

- **入门。**主要描述访问以太网交换机的方式和步骤。
- **端口。**主要介绍如何配置以太网端口、端口汇聚配置、端口镜像配置。
- **VLAN。**主要介绍 VLAN、isolate-user-vlan、GARP、GVRP 的相关配置。
- **组播协议。**主要介绍组播协议的配置，包括 IGMP snooping 配置、GMRP 的相关配置。
- **QoS/ACL。**主要介绍 QoS/ACL 的相关配置。
- **集中管理。**主要介绍以太网交换机集中管理的相关配置，包括堆叠配置等。
- **STP。**主要介绍以太网交换机上生成树协议的相关配置。
- **安全。**主要介绍以太网交换机安全相关配置，包括 802.1x、AAA、RADIUS 配置。

- **网络协议。**主要介绍 ARP、DHCP Snooping、IP 性能、访问管理等的配置。
- **系统管理。**主要介绍以太网交换机的管理和维护的相关配置，包括文件管理、系统维护、网络管理配置等。
- **典型组网案例。**主要介绍以太网交换机的组网配置实例等。
- **附录。**主要介绍交换网络的数据转发流程及本书中的缩略语等。

读者对象

本书适合下列人员阅读：

- 网络工程师
- 网络管理人员
- 具备网络基础知识的用户

本书约定

1. 通用格式约定

格　式	意　义
宋体	正文采用宋体表示。
黑体	除一级标题采用宋体**加粗**以外，其余各级标题均采用黑体。
楷体	警告、提示等内容一律用楷体，并且在内容前后增加线条与正文隔离。
“Terminal Display”格式	自定义的“Terminal Display”格式（英文 Courier New；中文 宋体；文字大小 8.5）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。

2. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
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。

格　式	意　义
{ 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。
#	由“#”号开始的行表示为注释行。

3. 键盘操作约定

格　式	意　义
加尖括号的字符	表示键名。如<Enter>、<Tab>、<Backspace>、<a>等分别表示回车、制表、退格、小写字母 a。
<键 1 + 键 2>	表示在键盘上同时按下几个键。如<Ctrl+Alt+A>表示同时按下“Ctrl”、“Alt”、“A”这三个键。
<键 1，键 2>	表示先按第一键，释放，再按第二键。如<Alt，F>表示先按<Alt>键，释放后再按<F>键。

4. 鼠标操作约定

格　式	意　义
单击	快速按下并释放鼠标的一个按钮。
双击	连续两次快速按下并释放鼠标的一个按钮。
拖动	按住鼠标的一个按钮不放，移动鼠标。

5. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

⚠ **小心、注意、警告、危险：**提醒操作中应注意的事项。

🕮 **说明、提示、窍门、思考：**对操作内容的描述进行必要的补充和说明。

目 录

第1章 产品介绍

1.1 产品简介

随着 Internet 市场的不断发展，用户对通信的需求已从传统的电话、传真、电报等低速业务逐渐向高速的 Internet 接入、可视电话、视频点播 VOD（Video On Demand）等宽带业务领域延伸，用户对上网速率的需求也越来越高。以太网接入因其成本低、使用简单、速度高而倍受市场的关注。面对迅猛发展的宽带网络建设需求，华为公司根据不同类型的客户需求，推出了 Quidway 系列以太网交换机。

Quidway S5000 系列以太网交换机是华为公司自主开发的 L2 层线速千兆以太网交换产品，是为企业网高速互连和千兆到桌面应用而设计的智能型可网管交换机。目前包含的型号为：

- S5012G 以太网交换机
- S5012T-12/10GBC 以太网交换机
- S5024G-24/20TP 以太网交换机

S5012G 以太网交换机提供 12 个 10/100/1000Base-T 自适应端口、4 个 Combo GBIC（Gigabit interface convertor）端口及 1 个 Console 口。

S5012T-12/10GBC 以太网交换机提供 10 个 GBIC 端口、2 个 10/100/1000Base-T 以太网端口、2 个 Combo 10/100/1000Base-T 以太网端口及 1 个 Console 口。

S5024G-24/20TP 以太网交换机提供 20 个 10/100/1000Base-T 以太网端口、4 个 GBIC 端口及 1 个 Console 口。

📖 **说明：**

Combo 端口的含义如下：
以 S5012G 以太网交换机为例，Combo GBIC 端口（端口号为 9+）与其对应的 10/100/1000BASE-T 以太网端口（端口号为 9）在逻辑上光电复用，用户可根据实际组网情况选择其一使用，但两者不能同时工作。

Quidway S5000 系列以太网交换机支持的业务如下：

- Internet 宽带接入
- 企业网和园区网组网

- 提供组播服务功能，支持组播音、视频服务

在本文中 Quidway S5000 系列以太网交换机简称为 S5000 系列以太网交换机。

1.2 功能特性列表

表1-1 功能特性列表

特性	说明
VLAN	支持符合 IEEE 802.1Q 标准的 VLAN（Virtual Local Area Network） 支持基于端口的 VLAN 支持 GVRP（GARP VLAN Registration Protocol）
生成树协议	支持 STP（Spanning Tree Protocol）/MSTP（Multiple Spanning Tree Protocol），符合 IEEE 802.1D/IEEE 802.1s 标准
流控	支持 IEEE 802.3x 流控（全双工） 支持背压式流控（半双工）
广播风暴抑制	支持广播风暴抑制
组播	支持 GMRP（GARP Multicast Registration Protocol） 支持 IGMP Snooping（Internet Group Management Protocol Snooping）
端口汇聚	支持端口汇聚
镜像	支持基于端口的镜像 支持基于流的镜像
QoS（Quality of Service）	支持的 QoS 如下： 支持流分类 支持带宽控制 支持优先级 支持端口优先级队列 队列调度：支持 SP（Strict Priority Queueing）、WRR（Weighted Round Robin）、RR（Round Robin）
安全特性	支持用户分级管理和口令保护 支持 802.1X 认证 支持包过滤

特性	说明
管理与维护	支持命令行接口配置 支持通过 Console 口进行配置 支持通过以太网端口利用 Telnet 或 SSH 进行配置 支持通过 Console 口利用 Modem 拨号进行配置 支持 SNMP 管理（支持华为 Quidview 网管系统，支持 RMON（Remote Monitoring）1，2，3，9 组 MIB） 支持系统日志 支持分级告警 支持 HGMP（Huawei Group Management Protocol）V2 支持调试信息输出 支持 PING、Tracert 支持通过 Modem 拨号、Telnet、SSH 进行远程维护
加载与升级	支持通过 XModem 协议实现加载升级 支持通过 FTP（File Transfer Protocol）、TFTP（Trivial File Transfer Protocol）实现加载升级

第2章 登录以太网交换机

2.1 通过 Console 口搭建配置环境

第一步：如图 2-1 所示，建立本地配置环境，只需将微机（或终端）的串口通过配置电缆与以太网交换机的 Console 口连接。

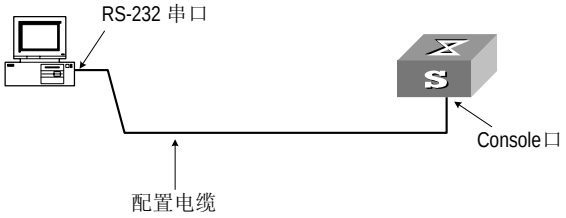


图2-1 通过 Console 口搭建本地配置环境

第二步：在微机上运行终端仿真程序（如 Windows 3.X 的 Terminal 或 Windows 9X 的超级终端等），设置终端通信参数为：波特率为 9600bit/s、8 位数据位、1 位停止位、无校验和无流控，并选择终端类型为 VT100，如图 2-2 至图 2-4 所示。

图2-2 新建连接

图2-3 连接端口设置

图2-4 端口通信参数设置

第三步：以太网交换机上电，终端上显示以太网交换机自检信息，自检结束后提示用户键入回车，之后将出现命令行提示符（如<Quidway>）。

第四步：键入命令，配置以太网交换机或查看以太网交换机运行状态。需要帮助可以随时键入“?”，具体的配置命令请参考本书中以后各章节的内容。

2.2 通过 Telnet 搭建配置环境

2.2.1 通过微机 Telnet 到以太网交换机

如果用户已经通过 Console 口正确配置以太网交换机管理 VLAN 接口的 IP 地址（在 VLAN 接口视图下使用 **ip address** 命令），并已指定与终端相连的以太网端口属于该管理 VLAN（在 VLAN 视图下使用 **port** 命令），这时可以利用 Telnet 登录到以太网交换机，然后对以太网交换机进行配置。

第一步：在通过 Telnet 登录以太网交换机之前，需要通过 Console 口在交换机上配置欲登录的 Telnet 用户名和认证口令。

🕮 **说明：**

Telnet 用户登录时，缺省需要进行口令认证，如果没有配置口令而通过 Telnet 登录，则系统会提示“password required, but none set.”。

<Quidway> system-view

```
Enter system view , return user view with Ctrl+Z.
```

[Quidway] user-interface vty 0

[Quidway-ui-vty0] set authentication password simple xxxx（xxxx 是欲设置的该 Telnet 用户登录口令）

第二步：如图 2-5 所示，建立配置环境，只需将微机以太网口通过局域网与以太网交换机的以太网口连接。

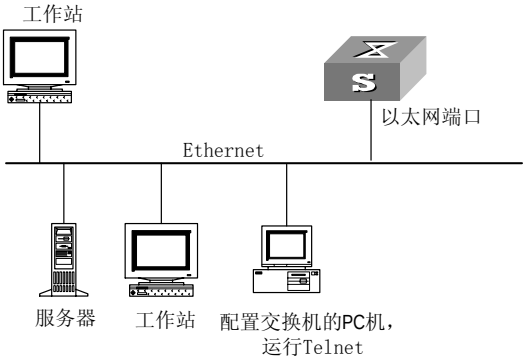


图2-5 通过局域网搭建本地配置环境

第三步：在微机上运行 Telnet 程序，输入与微机相连的以太网口所属 VLAN 的 IP 地址，如图 2-6 所示。

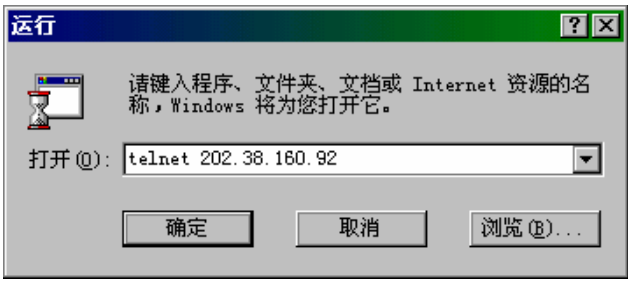


图2-6 运行 Telnet 程序

第四步：终端上显示“User Access Verification”，并提示用户输入已设置的登录口令，口令输入正确后则出现命令行提示符（如<Quidway>）。如果出现“Too many users!”的提示，表示当前 Telnet 到以太网交换机的用户过多，则请稍候再连（Quidway 系列以太网交换机最多允许 5 个 Telnet 用户同时登录）。

第五步：使用相应命令配置以太网交换机或查看以太网交换机运行状态。需要帮助可以随时键入“?”，具体的配置命令请参考本书中以后各章节的内容。

说明：

(1) 通过 Telnet 配置交换机时，不要删除或修改对应本 telnet 连接的交换机上的 VLAN 接口的 IP 地址，否则会导致 Telnet 连接断开。

(2) Telnet 用户登录时，缺省可以访问命令级别为 0 级的命令。

2.2.2 通过以太网交换机 Telnet 到以太网交换机

如果用户已经通过 Telnet 登录到一台交换机上，则可以通过该交换机 Telnet 到另一台交换机上进行配置。本交换机作为 Telnet 客户端，对端交换机作为 Telnet 服务器端。如果两台交换机相连的端口在同一局域网内，则其 IP 地址必须配置在同一网段；否则，两台交换机必须存在互相到达的路由。

配置环境如图 2-7 所示，用户 Telnet 到一台以太网交换机后，可以输入 **telnet** 命令再登录其它以太网交换机，对其进行配置管理。

图2-7 提供 Telnet Client 服务

第一步：先通过 Console 口在作为 Telnet Server 的交换机上配置欲登录的 Telnet 用户名和认证口令。

📖 说明：

Telnet 用户登录时，缺省需要进行口令认证，如果没有配置口令而通过 Telnet 登录，则系统会提示“password required, but none set.”。

<Quidway> system-view

```
Enter system view , return user view with Ctrl+Z.
```

[Quidway] user-interface vty 0

[Quidway-ui-vty0] set authentication password simple xxxx（xxxx 是欲设置的该 Telnet 用户登录口令）

第二步：用户登录到作为 Telnet Client 的以太网交换机（登录过程请参考本章“通过微机 Telnet 到以太网交换机”一节）。

第三步：在 Telnet Client 的以太网交换机上作如下操作：

<Quidway> telnet xxxx（xxxx 是作为 Telnet Server 的以太网交换机的主机名或 IP 地址，若为主机名，则交换机一定要有静态地址解析功能。）

第四步：输入已设置的登录口令，然后出现命令行提示符（如<Quidway>），如果出现“Too many users!”的提示，表示当前 Telnet 到以太网交换机的用户过多，则请稍候再连。

第五步：使用相应命令配置以太网交换机或查看以太网交换机运行状态。需要帮助可以随时键入“?”，具体的配置命令请参考本书中以后各章节的内容。

2.3 通过 Modem 拨号搭建配置环境

第一步：在通过 Modem 拨号登录以太网交换机之前，先通过 Console 口在以太网交换机上配置欲登录的 Modem 用户名和认证口令。

📖 说明：

Modem 用户登录时，缺省需要进行口令认证，如果没有配置口令而通过 Modem 登录，则系统会提示“password required, but none set.”。

<Quidway> system-view

```
Enter system view , return user view with Ctrl+Z.
```

[Quidway] user-interface aux 0

[Quidway-ui-aux0] set authentication password simple xxxx（xxxx 是欲设置的该 Modem 用户登录口令）

第二步：在与以太网交换机直接相连的 Modem 上进行以下配置（与终端相连的 Modem 不需要进行如下配置）。

```
AT&F      ---------------------- Modem 恢复出厂设置
ATS0=1    ---------------------- 设置自动应答（振铃一声）
AT&D      ---------------------- 忽略 DTR 信号
AT&K0     ---------------------- 禁止流量控制
AT&R1     ---------------------- 忽略 RTS 信号
AT&S0     ---------------------- 强制 DSR 为高电平
ATEQ1&W   ---------------------- 禁止 modem 回送命令响应和执行结果并存储配置
```

在配置后为了观察 Modem 的设置是否正确，可以输入 AT&V 命令显示配置的结果。

📖 **说明：**

(1) 各种 Modem 配置命令及显示的结果有可能不一样，具体操作请参照 Modem 的说明书进行。
(2) 建议 AUX（即 Console）口的传输速率要低于 Modem 的传输速率，否则可能会出现丢包现象。

第三步：如图 2-8 所示，建立远程配置环境，在微机（或终端）的串口和以太网交换机的 Console 口分别挂接 Modem。

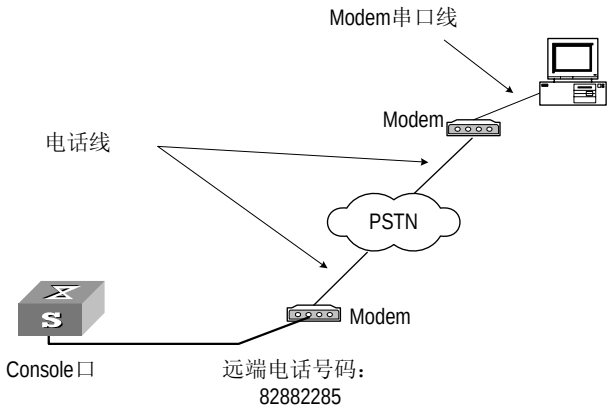


图2-8 搭建远程配置环境

第四步：在远端通过终端仿真程序和 Modem 向以太网交换机拨号（所拨号码应该是与以太网交换机相连的 Modem 的电话号码），与以太网交换机建立连接，如图 2-9 至 2-10 所示。

图2-9 拨号号码设置

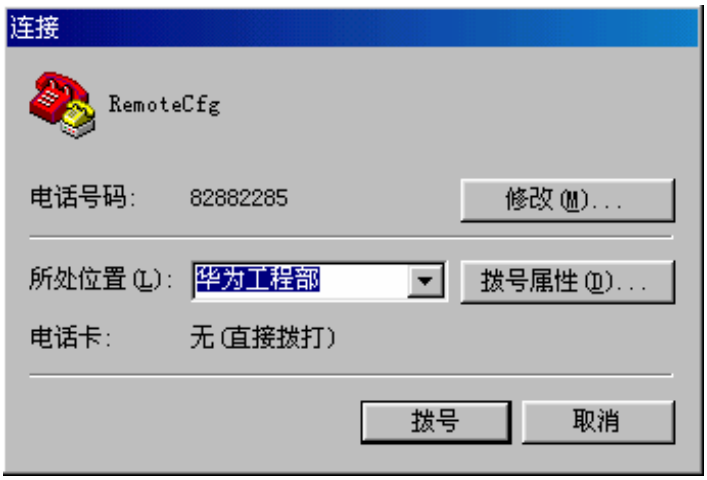


图2-10 在远端微机上拨号

第五步：在远端的终端仿真程序上输入已设置的登录口令，出现命令行提示符（如<Quidway>），即可对以太网交换机进行配置或管理。需要帮助可以随时键入“?”，具体的配置命令请参考本书中以后各章节的内容。

📖 **说明：**

Modem 用户登录时，缺省可以访问命令级别为 0 级的命令。

第3章 命令行接口

3.1 命令行接口

Quidway 系列以太网交换机向用户提供一系列配置命令以及命令行接口，方便用户配置和管理以太网交换机。命令行接口有如下特性：

- 通过 Console 口进行本地配置。
- 通过 Telnet 或 SSH 进行本地或远程配置。
- 通过 Modem 拨号登录到以太网交换机进行远程配置。
- 配置命令分级保护，确保未授权用户无法侵入以太网交换机。
- 用户可以随时键入<?>以获得在线帮助。
- 提供网络测试命令，如 Tracert、Ping 等，迅速诊断网络是否正常。
- 提供种类丰富、内容详尽的调试信息，帮助诊断网络故障。
- 用 Telnet 命令直接登录并管理其它以太网交换机。
- 提供 FTP 服务，方便用户上载、下载文件。
- 提供类似 Doskey 的功能，可以执行某条历史命令。
- 命令行解释器对关键字采取不完全匹配的搜索方法，用户只需键入无冲突关键字即可解释。

3.2 命令行视图

Quidway 系列以太网交换机的命令行采用分级保护方式，防止未授权用户的非法侵入。

命令行划分为参观级、监控级、配置级、管理级 4 个级别，简介如下：

- 参观级：该级别包含的命令有网络诊断工具命令（**ping**、**tracert**）、用户界面的语言模式切换命令（**language-mode**）以及 **telnet** 命令等，该级别命令不允许进行配置文件保存的操作。
- 监控级：用于系统维护、业务故障诊断等，包括 **display**、**debugging** 命令，该级别命令不允许进行配置文件保存的操作。
- 配置级：业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。

- 管理级：关系到系统基本运行，系统支撑模块的命令，这些命令对业务提供支撑作用，包括文件系统、FTP、TFTP、XModem 下载、用户管理命令、级别设置命令等。

同时对登录用户也划分为 4 个级别，分别与命令级别相对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。

为了防止未授权用户的非法侵入，用户在使用 **super** [*level*]命令从低级别切换到高级别时，要进行用户身份验证，即需要输入切换口令（如果用户已经使用命令 **super password** [**level** *level*] { **simple** | **cipher** } *password* 设置了切换口令）。为了保密，用户在屏幕上看不到所键入的口令，如果三次以内输入正确的口令，则切换到高级别用户，否则保持原用户级别不变。

各命令行视图是针对不同的配置要求实现的，它们之间有联系又有区别，比如，与以太网交换机建立连接即进入用户视图，它只完成查看运行状态和统计信息的简单功能，再键入 **system-view** 进入系统视图，在系统视图下，可以键入不同的命令进入相应的视图。

命令行提供如下视图：

- 用户视图
- 系统视图
- 以太网端口视图
- VLAN 视图
- VLAN 接口视图
- 本地用户视图
- 用户界面视图
- FTP Client 视图
- 集群视图
- MST 域视图
- 公共密钥视图
- 公共密钥编辑视图
- 基本 ACL 视图
- 高级 ACL 视图
- 二层 ACL 视图
- RADIUS 服务器组视图
- ISP 域视图

视图关系简图如图 3-1 所示：

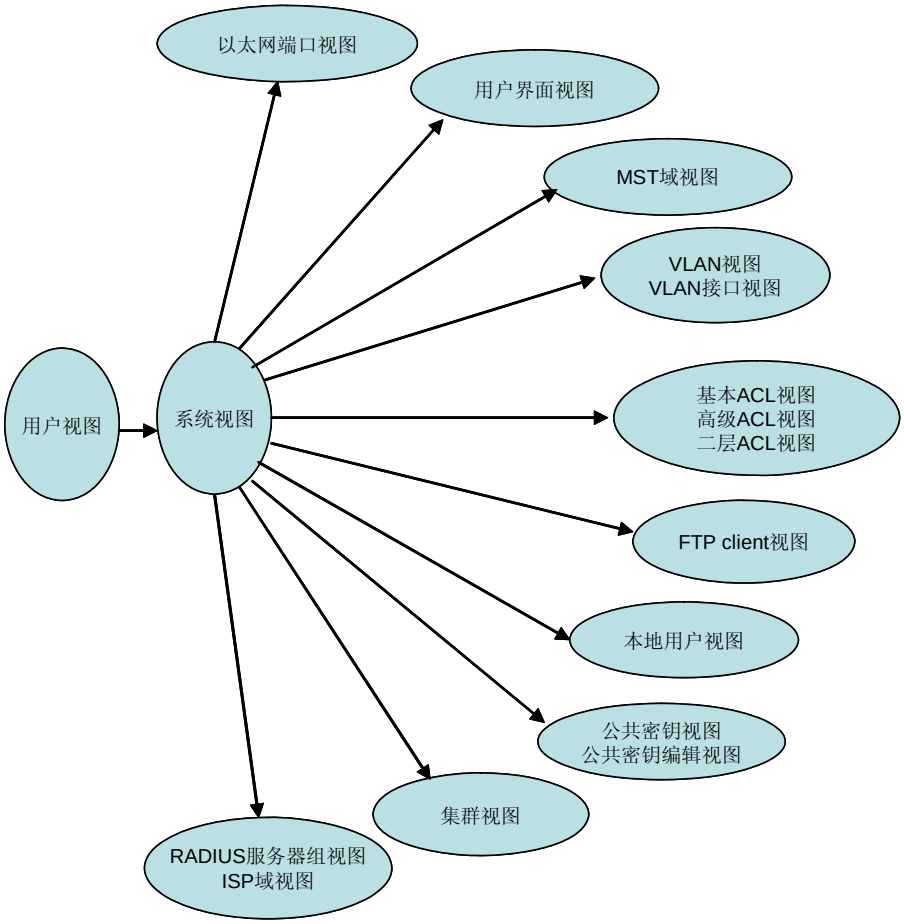


图3-1 视图关系简图

各命令视图的功能特性、进入各视图的命令等细则如表 3-1 所示。

表3-1 命令视图功能特性列表

视图	功能	提示符	进入命令	退出命令
用户视图	查看交换机的简单运行状态和统计信息	<Quidway>	与交换机建立连接即进入	**quit** 断开与交换机连接
系统视图	配置系统参数	[Quidway]	在用户视图下键入 **system-view**	**quit** 或 **return** 返回用户视图
以太网端口视图	配置以太网端口参数	[Quidway-GigabitEthernet0/1]	在系统视图下键入：**interface gigabitethernet** 0/1	**quit** 返回系统视图
VLAN 视图	配置 VLAN 参数	[Quidway-Vlan1]	在系统视图下键入 **vlan** 1	**quit** 返回系统视图

视图	功能	提示符	进入命令	退出命令
VLAN 接口视图	配置 VLAN 和 VLAN 汇聚对应的 IP 接口参数	[Quidway-Vlan-interface1]	在系统视图下键入：**interface vlan-interface** 1	**quit** 返回系统视图
本地用户视图	配置本地用户参数	[Quidway-luser-user1]	在系统视图下键入：**local-user** user1	**quit** 返回系统视图
用户界面视图	配置用户界面参数	[Quidway-ui0]	在系统视图下键入 **user-interface** 0	**quit** 返回系统视图
FTP Client 视图	配置 FTP Client 参数	[ftp]	在用户视图下键入 **ftp**	**quit** 返回用户视图
集群视图	配置集群参数	[Quidway-cluster]	在系统视图下键入 **cluster**	**quit** 返回系统视图
MST 域视图	配置 MST 域的参数	[Quidway-mst-region]	在系统视图下键入 **stp region-configuration**	**quit** 返回系统视图
公共密钥视图	配置 SSH 用户的 RSA 公共密钥	[Quidway-rsa-public-key]	在系统视图下键入 **rsa peer-public-key** quidway003	**peer-public-key end** 返回系统视图
公共密钥编辑视图	编辑 SSH 用户的 RSA 公共密钥	[Quidway-rsa-key-code]	在公共密钥视图下键入 **public-key-code begin**	**public-key-code end** 返回公共密钥视图
基本 ACL 视图	定义基本 ACL 的子规则	[Quidway-acl-basic-2000]	在系统视图下键入 **acl number** 2000	**quit** 返回系统视图
高级 ACL 视图	定义高级 ACL 的子规则	[Quidway-acl-adv-3000]	在系统视图下键入 **acl number** 3000	**quit** 返回系统视图
二层 ACL 视图	定义二层 ACL 的子规则	[Quidway-acl-link-4000]	在系统视图下键入 **acl number** 4000	**quit** 返回系统视图
RADIUS 服务器组视图	配置 Radius 协议参数	[Quidway-radius-1]	在系统视图下键入 **radius scheme** 1	**quit** 返回系统视图
ISP 域视图	配置 ISP 域的相关属性	[Quidway-isp-huawei163.net]	在系统视图下键入 **domain** huawei163.net	**quit** 返回系统视图

3.3 命令行特性

3.3.1 命令行在线帮助

命令行接口提供如下几种在线帮助：

- 完全帮助
- 部分帮助

通过上述各种在线帮助能够获取到帮助信息，分别描述如下：

(1) 在任一视图下，键入<?>获取该视图下所有的命令及其简单描述。

<Quidway> ?

```
User view commands:
  language-mode  Specify the language environment
  ping           Ping function
  quit           Exit from current command view
  super          Privilege specified user priority level
  telnet         Establish one TELNET connection
  tracert        Trace route function
```

(2) 键入一命令，后接以空格分隔的<?>，如果该位置为关键字，则列出全部关键字及其简单描述。

<Quidway> language-mode ?

```
  chinese  Chinese environment
  english  English environment
```

(3) 键入一命令，后接以空格分隔的<?>，如果该位置为参数，则列出有关的参数描述。

[Quidway] garp timer leaveall ?

```
  INTEGER<65-32765>  Value of timer in centiseconds
                     (LeaveAllTime > (LeaveTime [On all ports]))
                     Time must be multiple of 5 centiseconds
```

[Quidway] garp timer leaveall 300 ?

```
  <cr>
```

<cr>表示该位置无参数，在紧接着的下一个命令行该命令被复述，直接键入回车即可执行。

(4) 键入一字符串，其后紧接<?>，列出以该字符串开头的所有命令。

<Quidway> p?

```
ping
```

(5) 键入一命令，后接一字符串紧接<?>，列出命令以该字符串开头的所有关键字。

<Quidway> display ver?

version

(6) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字。

(7) 以上帮助信息，均可通过执行 **language-mode** 命令切换为中文显示。

3.3.2 命令行显示特性

命令行接口提供了如下的显示特性：

- 为方便用户，提示信息和帮助信息可以用中英文两种语言显示。
- 在一次显示信息超过一屏时，提供了暂停功能，这时用户可以有三种选择，如表 3-2 所示。

表3-2 显示功能表

按键或命令	功能
暂停显示时键入<Ctrl+C>	停止显示和命令执行
暂停显示时键入空格键	继续显示下一屏信息
暂停显示时键入回车键	继续显示下一行信息

3.3.3 命令行历史命令

命令行接口提供类似 Doskey 功能，将用户键入的历史命令自动保存，用户可以随时调用命令行接口保存的历史命令，并重复执行。命令行接口为每个用户缺省保存 10 条历史命令。操作如表 3-3 所示。

表3-3 访问历史命令

操作	按键	结果
显示历史命令	**display history-command**	显示用户输入的历史命令
访问上一条历史命令	上光标键↑或<Ctrl+P>	如果还有更早的历史命令，则取出上一条历史命令
访问下一条历史命令	下光标键↓或<Ctrl+N>	如果还有更晚的历史命令，则取出下一条历史命令

说明：

用光标键对历史命令进行访问，在 Windows 3.X 的 Terminal 和 Telnet 下都是有效的，但对于 Windows 9X 超级终端，↑、↓光标键会无效，这是由于 Windows 9X 的超级终端对这两个键作了不同解释所致，这时可以用组合键<Ctrl+P>和<Ctrl+N>来代替↑、↓光标键达到同样目的。

3.3.4 命令行错误信息

所有用户键入的命令，如果通过语法检查，则正确执行，否则向用户报告错误信息，常见错误信息参见表 3-4。

表3-4 命令行常见错误信息表

英文错误信息	错误原因
Unrecognized command	没有查找到命令
	没有查找到关键字
	参数类型错
	参数值越界
Incomplete command	输入命令不完整
Too many parameters	输入参数太多
Ambiguous command	输入参数不明确

3.3.5 命令行编辑特性

命令行接口提供了基本的命令编辑功能，支持多行编辑，每条命令的最大长度为 256 个字符，如表 3-5 所示。

表3-5 编辑功能表

按键	功能
普通按键	若编辑缓冲区未满，则插入到当前光标位置，并向右移动光标
退格键 Backspace	删除光标位置的前一个字符，光标前移
左光标键←或<Ctrl+B>	光标向左移动一个字符位置
右光标键→或<Ctrl+F>	光标向右移动一个字符位置

按键	功能
上光标键↑或<Ctrl+P> 下光标键↓或<Ctrl+N>	显示历史命令
Tab 键	输入不完整的关键字后按下 Tab 键，系统自动执行部分帮助：如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入并换行显示；对于命令字的参数、不匹配或者匹配的关键字不唯一的情况，系统不作任何修改，重新换行显示原输入。

第4章 用户界面配置

4.1 用户界面简介

用户界面配置是以太网交换机提供的另一种配置方法，用来配置和管理端口属性，方便用户管理。

目前 S5000 系列以太网交换机支持的配置方式有：

- 通过 Console 口本地配置
- 通过以太网端口利用 Telnet 或 SSH 进行本地或远程登录配置
- 通过 Console 口利用 Modem 拨号进行远程配置

与这些配置方式对应的是两种类型的用户界面：

- AUX 用户界面（AUX）

AUX 用户界面用于通过 Console 口对以太网交换机进行访问，每台以太网交换机最多只有一个。

- VTY 用户界面（VTY）

VTY 用户界面用于通过 Telnet 对以太网交换机进行访问，每台交换机最多可以有 5 个。

📖 **说明：**

在 Quidway 系列以太网交换机中，AUX 口和 Console 口是同一个口，所以用户界面类型中只有 AUX 口用户界面类型。

用户界面的编号有两种方式：绝对编号方式和相对编号方式。

(1) 绝对编号方式，遵守的规则如下：

- AUX 用户界面编号排在第一位，为 0；
- VTY 用户界面排在 AUX 用户界面之后。第一个 VTY 的绝对编号比 AUX 大 1。

(2) 相对编号的形式是：用户界面类型＋编号。此编号是每种类型的用户界面的编号。遵守的规则如下：

- AUX 用户界面的编号：aux 0；
- VTY 用户界面的编号：第一条为 vty 0，第二条为 vty 1，依此类推。

4.2 用户界面配置

用户界面配置包括：

- 进入用户界面视图
- 配置用户界面支持的协议
- 配置 AUX（即 Console）口属性
- 配置终端属性
- 用户管理
- 配置重定向功能

4.2.1 进入用户界面视图

可以通过下面的命令进入相应的用户界面视图。可以进入单一用户界面视图对一个用户界面进行配置，也可以进入多个用户界面视图同时配置多个用户界面。

请在系统视图下进行下列配置。

表4-1 进入用户界面视图

操作	命令
进入单一用户界面视图或多个用户界面视图	**user-interface** [*type*] *first-number* [*last-number*]

4.2.1 配置用户界面支持的协议

可以使用下面的命令设置用户界面支持的协议，系统将只允许通过所支持的协议登录该用户界面。配置结果在下次登录请求时生效。

请在用户界面视图下进行下列配置（只能在 VTY 用户界面视图下进行）。

表4-2 配置用户界面支持的协议

操作	命令
配置用户界面支持的协议	**protocol inbound** { **all** | **ssh** | **telnet** }

缺省情况下，系统只支持 Telnet 协议。

注意：

(1) 如果配置用户界面支持 Telnet 协议，则由于用户登录时缺省需要进行口令认证，故需要用户配置口令才能成功登录。

(2) 如果配置用户界面支持 SSH 协议，则为确保登录成功，请您务必配置相应的认证方式为 **authentication-mode scheme**；若配置认证方式为 **authentication-mode password** 和 **authentication-mode none**，则 **protocol inbound ssh** 配置结果将失败。反之亦然，如果某用户界面已经配置成支持 SSH 协议，则在此用户界面上 **authentication-mode password** 和 **authentication-mode none** 的配置将失败。

4.2.2 配置 AUX（即 Console）口属性

可以通过下面的命令配置 AUX（即 Console）口的属性，包括速率、流控方式、校验方式、停止位、数据位。

请在用户界面视图下进行下列配置（只能在 AUX 用户界面视图下进行）。

1. 配置 AUX（即 Console）口的传输速率

表4-3 配置 AUX（即 Console）口的传输速率

操作	命令
配置 AUX（即 Console）口的传输速率	**speed** *speed-value*
恢复 AUX（即 Console）口的传输速率为缺省值	**undo speed**

缺省情况下，AUX（即 Console）口支持的传输速率为 9600bit/s。

2. 配置 AUX（即 Console）口的流控方式

表4-4 配置 AUX（即 Console）口的流控方式

操作	命令
配置 AUX（即 Console）口的流控方式	**flow-control** { **hardware** | **none** | **software** }
恢复 AUX（即 Console）口的流控方式为缺省方式	**undo flow-control**

缺省情况下，AUX（即 Console）口的流控方式为 none，即不进行流控。

3. 配置 AUX（即 Console）口的校验方式

表4-5 配置 AUX（即 Console）口的校验方式

操作	命令
配置 AUX（即 Console）口的校验方式	**parity** { **even** | **mark** | **none** | **odd** | **space** }
恢复 AUX（即 Console）口的校验方式为缺省方式	**undo parity**

缺省情况下，AUX（即 Console）口的校验方式为 none，即无校验位。

4. 配置 AUX（即 Console）口的停止位

表4-6 配置 AUX（即 Console）口的停止位

操作	命令
配置 AUX（即 Console）口的停止位	**stopbits** { **1** | **1.5** | **2** }
恢复 AUX（即 Console）口的停止位为缺省值	**undo stopbits**

缺省情况下，AUX（即 Console）口的停止位为 1。

5. 配置 AUX（即 Console）口的数据位

表4-7 配置 AUX（即 Console）口的数据位

操作	命令
配置 AUX（即 Console）口的数据位	**databits** { **7** | **8** }
恢复 AUX（即 Console）口数据位为缺省值	**undo databits**

缺省情况下，AUX（即 Console）口支持的数据位为 8 位。

4.2.3 配置终端属性

可以通过下面的命令配置终端属性，包括启动/关闭终端服务、超时断开设定、锁住用户界面、配置终端屏幕的一屏行数以及配置历史命令缓冲区大小。

请在用户界面视图下进行下列配置，其中锁住用户界面操作请在用户视图下进行。

1. 启动/关闭终端服务

当关闭某用户界面的终端服务后，通过该用户界面将不能登录以太网交换机。对于在关闭之前已经通过该用户界面登录的用户，仍然可以进行操作。但当用户退出该用户界面后，将不能再次登录。只有启动该用户界面的终端服务后，才能通过该用户界面登录以太网交换机。

表4-8 启动/关闭终端服务

操作	命令
启动终端服务	**shell**
关闭终端服务	**undo shell**

缺省情况下，在所有的用户界面上启动终端服务。

需要注意的是：

- 因为 AUX（即 Console）口本身就是配置口，为了安全起见，**undo shell** 命令在 AUX（即 Console）口不支持，其它用户界面均支持。
- 用户不能在自己登录的用户界面上使用本命令。
- 在任何合法的用户界面上使用 **undo shell** 命令，都需要经过用户的确认。

2. 超时断开设定

表4-9 设置用户超时断连功能

操作	命令
设置用户超时断连功能	**idle-timeout** *minutes* [*seconds*]
恢复用户超时断连为缺省值	**undo idle-timeout**

缺省情况下，在所有的用户界面上启动了超时断连功能，时间为 10 分钟。也就是说，如果 10 分钟内某用户界面没有用户进行操作，则该用户界面将自动断开。

idle-timeout 0 表示关闭超时中断连接功能。

3. 设置锁住用户界面

该配置任务用来锁住当前使用的用户界面，并提示用户输入密码。防止当用户离开时，其它人对该用户界面进行操作。

表4-10 设置锁住用户界面

操作	命令
锁住用户界面	**lock**

4. 设置终端屏幕的一屏行数

当某命令显示信息的行数多于一屏中能够显示的范围时，可以使用以下命令设置一屏中可以显示的行数，以便将信息分成几段，方便查看。

表4-11 设置终端屏幕的一屏行数

操作	命令
设置终端屏幕的一屏行数	**screen-length** *screen-length*
恢复终端屏幕一屏行数为缺省值	**undo screen-length**

缺省情况下，终端屏幕一屏行数为 24 行。

screen-length 0 表示关闭分屏功能。

5. 设置历史命令缓冲区大小

表4-12 设置历史命令缓冲区大小

操作	命令
设置历史命令缓冲区大小	**history-command max-size** *value*
恢复历史命令缓冲区大小为缺省值	**undo history-command max-size**

缺省情况下，历史缓冲区为 10，即可存放 10 条历史命令。

4.2.4 用户管理

用户管理包括用户登录验证方式的设置、用户登录后可以访问的命令级别的设置、从用户界面登录后可以访问的命令级别的设置以及命令级别的设置。

1. 设置用户登录验证方式

可以使用以下命令设置用户登录时是否需要进行验证，以防止非法用户的侵入。

请在用户界面视图下进行下列配置。

表4-13 设置用户登录验证方式

操作	命令
设置登录用户的认证方式	**authentication-mode** { **password** | **scheme** }
设置认证方式为不验证	**authentication-mode none**

缺省情况下，Console 口用户登录不需要进行终端验证；而 Telnet 和 Modem 用户登录需要进行口令验证。

(1) 本地口令验证

使用 **authentication-mode password** 命令，表示需要进行本地口令认证，此时需要使用以下命令配置口令后，才能成功登录。

请在用户界面视图下进行下列配置。

表4-14 设置本地验证的口令

操作	命令
设置本地验证的口令	**set authentication password** { **cipher** | **simple** } *password*
取消本地验证的口令	**undo set authentication password**

设置用户从 VTY 0 用户界面登录时需要进行口令验证，且验证口令为 huawei。

[Quidway] user-interface vty 0

[Quidway-ui-vty0] authentication-mode password

[Quidway-ui-vty0] set authentication password simple huawei

(2) 本地或远端用户名和口令验证

使用 **authentication-mode scheme** 命令，表示需要进行本地或远端用户名和口令认证。究竟是采用本地认证还是远端认证视配置而定，详细内容请见“安全”模块的介绍。

下面仅以本地用户名和口令认证为例介绍配置过程。

设置用户从 VTY 0 用户界面登录时需要进行用户名和口令验证，且登录用户名和口令分别为 zbr 和 huawei。

[Quidway-ui-vty0] authentication-mode scheme

[Quidway-ui-vty0] quit

[Quidway] local-user zbr

[Quidway-luser-zbr] password simple huawei

[Quidway-luser-zbr] service-type telnet

(3) 不验证

[Quidway-ui-vty0] authentication-mode none

📖 **说明：**

Modem 和 Telnet 用户登录时，缺省需要进行口令认证，如果没有配置口令而登录，则系统会提示“password required, but none set.”。

如果使用 **authentication-mode none** 命令，则 Modem 和 Telnet 用户登录时不需要进行口令的验证。

---

2. 设置用户登录后可以访问的命令级别

可以使用以下的命令设置某用户登录后可以访问的命令级别。

请在本地用户视图下进行下列配置。

表4-15 设置用户登录后可以访问的命令级别

操作	命令
设置指定用户登录后可以访问的命令级别	**service-type** { **ssh** [**level** *level* | **telnet** [**level** *level*]] | **telnet** [**level** *level* | **ssh** [**level** *level*]] }
恢复指定用户登录后可以访问的命令级别为缺省级别	**undo service-type** { **ssh** [**level** | **telnet** [**level**]] | **telnet** [**level** | **ssh** [**level**]] }

缺省情况下，指定用户登录可以访问的命令级别为 1 级。

3. 设置从用户界面登录后可以访问的命令级别

可以使用以下命令设置从某用户界面登录后可以访问的命令级别，执行该级别范围内的命令。

请在用户界面视图下进行下列配置。

表4-16 设置从用户界面登录后可以访问的命令级别

操作	命令
设置从用户界面登录后可以访问的命令级别	**user privilege level** *level*
恢复从用户界面登录后可以访问的命令级别为缺省级别	**undo user privilege level**

缺省情况下，从 AUX 用户界面登录后可以访问的命令级别为 3 级，从 VTY 用户界面登录后可以访问的命令级别为 0 级。

📖 说明：

用户登录以太网交换机时，其所能访问的命令级别取决于用户自身可以访问的命令级别与从用户界面登录所能访问的命令级别的设置，如果两者不同，则以用户自身可以访问的命令级别为准。例如：某用户可以访问的命令级别是 3 级，而从 VTY 0 用户界面登录所能访问的命令级别是 1 级，则该用户从 VTY 0 登录系统时，可以访问 3 级及以下的命令。

4. 设置命令的级别

可以使用以下命令设置指定视图内指定命令的级别。命令权限共分为参观、监控、配置、管理 4 个级别，分别对应标识 0、1、2、3。管理员可以根据用户需要指定命令权限。

请在系统视图下进行下列操作。

表4-17 设置命令的级别

操作	命令
设置指定视图中指定命令的级别	**command-privilege level** *level* **view** *view command*
恢复指定视图中指定命令的级别为缺省值	**undo command-privilege view** *view command*

📖 说明：

请用户不要轻易改变命令级别，否则可能带来维护和操作上的不便。

4.2.5 配置重定向功能

1. 传递命令

可以通过下面的命令实现用户界面之间传递消息的功能。

请在用户视图下进行下列配置。

表4-18 设置在用户界面之间传递消息

操作	命令
设置在用户界面之间传递消息	**send** { **all** | *number* | *type number* }

2. 自动执行命令

可以通过下面的命令配置登录时自动执行命令。某条命令被配置为自动执行后，当用户重新登录时，系统将自动执行该命令。

通常的用法是在终端使用以下命令配置 **telnet** 命令，使用户自动连接到指定的设备。

请在用户界面视图下进行下列配置。

表4-19 设置自动执行命令

操作	命令
设置自动执行命令	**auto-execute command** *text*
取消自动执行命令	**undo auto-execute command**

需要注意的是：

- 该命令的使用将导致不能使用该用户界面对本系统进行常规的配置，需谨慎使用。
- 在配置 **auto-execute command** 命令并保存配置（执行 **save** 操作）之前，要确保可以通过其它手段登录系统以去掉此配置。

配置用户从 VTY 0 上登录后，自动执行 telnet 10.110.100.1 命令。

[Quidway-ui-vty0] auto-execute command telnet 10.110.100.1

当用户从 VTY 0 登录时，将自动执行 **telnet** 10.110.100.1 命令。

4.3 用户界面显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后用户界面的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **free** 命令可以清除用户界面的信息。

表4-20 用户界面显示和调试

操作	命令
清除指定的用户界面	**free user-interface** [*type*] *number*
显示用户界面的使用信息	**display users** [**all**]
显示用户界面的物理属性和一些配置	**display user-interface** [*type number*] [*number*]

第5章 系统 IP 配置

5.1 系统 IP 简介

5.1.1 管理 VLAN

如果要对以太网交换机进行 Telnet、网管等远程管理，必须通过设置交换机的 IP 地址才能实现。Quidway 系列二层以太网交换机同时只能有一个 VLAN 对应的 VLAN 接口可以配置 IP 地址，而该 VLAN 即为管理 VLAN。

5.1.2 IP 地址

1. IP 地址的分类和表示

IP 地址是分配给连接在 Internet 上的设备的一个 32 比特长度的地址。IP 地址由两个字段组成：网络号码字段（net-id）和主机号码字段（host-id）。IP 地址由美国国防数据网的网络信息中心（NIC）进行分配。为了方便 IP 地址的管理，IP 地址分成五类。如下图所示：

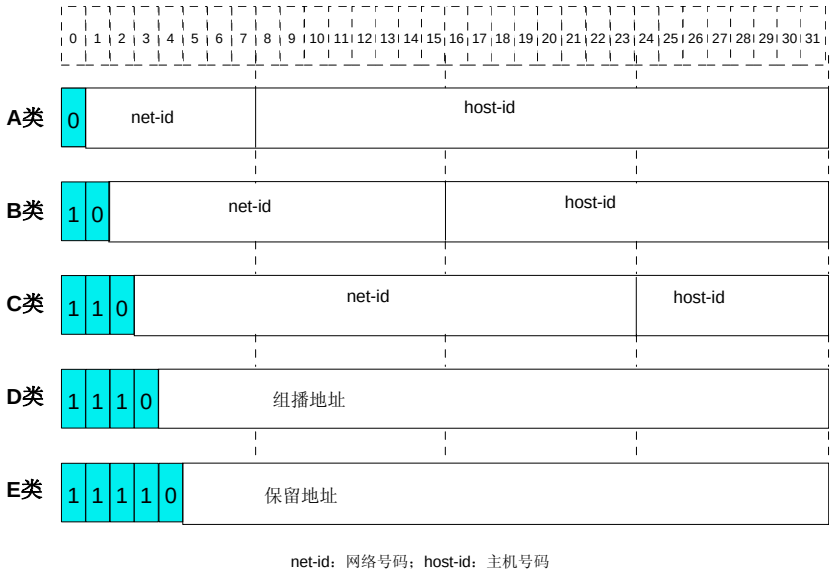


图5-1 五类 IP 地址

其中 A、B、C 类地址为单播（unicast）地址；D 类地址为组播（multicast）地址；E 类地址为保留地址，以备将来的特殊用途。目前大量使用中的 IP 地址属于 A、B、C 三类地址。

IP 地址采用点分十进制方式记录。每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.110.50.101。

在使用 IP 地址时要知道一些 IP 地址是保留作为特殊用途的，一般不使用。下表列出用户可配置的 IP 地址范围。

表5-1 IP 地址分类及范围

网络类型	地址范围	用户可用的 IP 网络范围	说明
A	0.0.0.0 ～ 127.255.255.255	1.0.0.0 ～ 126.0.0.0	全 0 的主机号码表示该 IP 地址就是网络的地址，用于网络路由； 全 1 的主机号码表示广播地址，即对该网络上所有的主机进行广播； IP 地址 0.0.0.0 用于启动后不再使用的主机； 网络号码为 0 的 IP 地址表示当前网络，可以让机器引用自己的网络而不必知道其网络号； 所有形如 127.X.Y.Z 的地址都保留作回路测试，发送到这个地址的分组不会输出到线路上，它们被内部处理并当作输入分组。
B	128.0.0.0 ～ 191.255.255.255	128.0.0.0 ～ 191.254.0.0	全 0 的主机号码表示该 IP 地址就是网络的地址，用于网络路由； 全 1 的主机号码表示广播地址，即对该网络上所有的主机进行广播。
C	192.0.0.0 ～ 223.255.255.255	192.0.0.0 ～ 223.255.254.0	全 0 的主机号码表示该 IP 地址就是网络的地址，用于网络路由； 全 1 的主机号码表示广播地址，即对该网络上所有的主机进行广播。
D	224.0.0.0 ～ 239.255.255.255	无	D 类地址是一种组播地址。
E	240.0.0.0 ～ 255.255.255.254	无	保留今后使用。
其它地址	255.255.255.255	255.255.255.255	255.255.255.255 用于局域网广播地址。

2. 子网和掩码

在 Internet 迅速发展的今天，IP 地址消耗殆尽。而传统的 IP 地址分配方式，对 IP 地址的浪费非常严重。为了充分利用已有的 IP 地址，人们提出了地址掩码（mask）和子网（subnet）的概念。

掩码是一个 IP 地址对应的 32 位数字，这些数字中一些为 1，另外一些为 0。原则上这些 1 和 0 可以任意组合，不过一般在设计掩码时，把掩码开始连续的几位设置为 1。掩码可以把 IP 地址分为两个部分：子网地址和主机地址。IP 地址与掩码中为 1 的位对应的部分为子网地址，其他的位则是主机地址。当不进行子网划分时，子网掩码即为默认值，此时子网掩码中“1”的长度就是网络号码的长度。即 A 类地址对应的掩码默认值为 255.0.0.0；B 类地址的掩码默认值为 255.255.0.0；C 类地址的掩码的默认值为 255.255.255.0。

使用掩码把一个可以包括 1600 多万主机的 A 类网络或 6 万多台主机的 B 类网络分割成许多小的网络，每一个小的网络就称之为子网。如一个 B 类网络地址 202.38.0.0 就可以利用掩码 255.255.224.0，把该网络分为 8 个子网：202.38.0.0 、 202.38.32.0 、 202.38.64.0 、 202.38.96.0 、 202.38.128.0, 202.38.160.0、202.38.192.0、202.38.224.0（请参见下图），而每个子网可以包括 8000 多台主机。

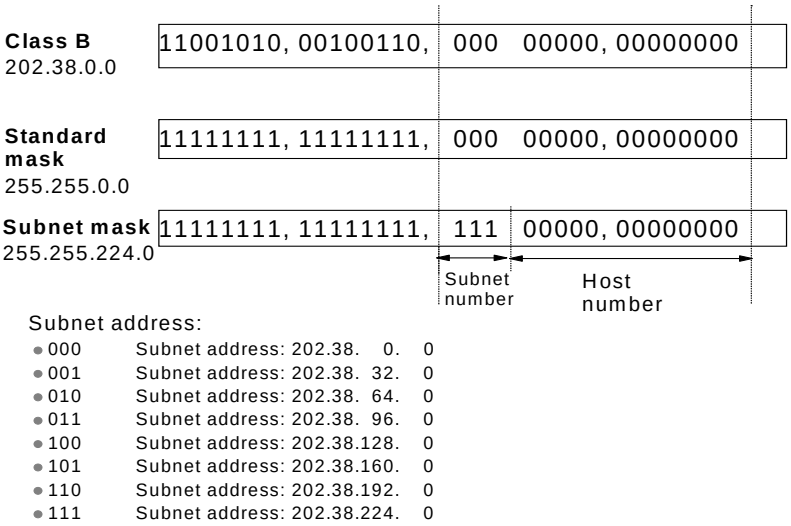


图5-2 IP 地址子网划分

5.1.3 静态路由

静态路由是一种由网络管理员手工设置的路由。静态路由应用于组网结构比较简单的网络中。合理设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

华为二层系列以太网交换机可以配置静态路由，用于通过网络对交换机进行访问。

5.2 系统 IP 配置

系统 IP 配置包括：

- 创建/删除管理 VLAN 接口
- 为管理 VLAN 接口指定/删除 IP 地址
- 为管理 VLAN 接口指定描述字符
- 打开/关闭管理 VLAN 接口
- 配置主机名和对应的 IP 地址
- 配置静态路由
- 配置静态路由的缺省优先级

5.2.1 创建/删除管理 VLAN 接口

请在系统视图下进行下列配置。

表5-2 创建/删除管理 VLAN 接口

操作	命令
创建并进入管理 VLAN 接口视图	**interface vlan-interface** *vlan-id*
删除管理 VLAN 接口	**undo interface vlan-interface** *vlan-id*

需要注意的是，在本配置任务之前要先创建对应 *vlan-id* 的 VLAN。但 VLAN1 是缺省的 VLAN，不需创建。

5.2.2 为管理 VLAN 接口指定/删除 IP 地址

可以使用以下命令为管理 VLAN 接口指定 IP 地址，从而可以实现对以太网交换机进行 Telnet、网管等远程管理。

请在 VLAN 接口视图下进行下列配置。

表5-3 为管理 VLAN 接口指定/删除 IP 地址

操作	命令
配置管理 VLAN 接口 IP 地址	**ip address** *ip-address net-mask*
删除管理 VLAN 接口 IP 地址	**undo ip address** [*ip-address net-mask*]

缺省情况下，管理 VLAN 接口无 IP 地址。

5.2.3 为管理 VLAN 接口指定描述字符

可以使用下面的命令来指定管理 VLAN 接口的描述字符。

请在 VLAN 接口视图下进行下列配置。

表5-4 为管理 VLAN 接口指定描述字符

操作	命令
为管理 VLAN 接口指定一个描述字符串	**description** *string*
恢复管理 VLAN 接口的描述字符串为缺省描述	**undo description**

缺省情况下，管理 VLAN 接口的描述字符串为“HUAWEI, Quidway Series, Vlan-interface1 Interface”，其中 Vlan-interface1 是管理 VLAN 接口的接口名。

5.2.4 打开/关闭管理 VLAN 接口

当管理 VLAN 接口的相关参数及协议配置好之后，可以使用下面的命令打开管理 VLAN 接口；如果不想管理 VLAN 接口起作用，则可以使用下面的命令关闭管理 VLAN 接口。

请在 VLAN 接口视图下进行下列配置。

表5-5 打开或关闭管理 VLAN 接口

操作	命令
关闭管理 VLAN 接口	**shutdown**
打开管理 VLAN 接口	**undo shutdown**

需要注意的是，打开/关闭管理 VLAN 接口的操作对属于该管理 VLAN 的以太网端口的打开/关闭状态没有影响。

缺省情况下，当管理 VLAN 接口对应 VLAN 下的所有以太网端口状态为 down 时，管理 VLAN 接口为 down 状态，即关闭状态；当管理 VLAN 接口对应 VLAN 下有一个或一个以上的以太网端口处于 up 状态，VLAN 接口处于 up 状态，即打开状态。

5.2.5 配置主机名和对应的 IP 地址

用户可以使用本命令将主机名与主机 IP 地址相对应，当用户使用 telnet 等应用时，可以直接使用主机名，由系统解析为 IP 地址，而不必使用难于记忆的 IP 地址。

请在系统视图下进行下列配置。

表5-6 配置主机名和对应的 IP 地址

操作	命令
配置主机名和对应的 IP 地址	**ip host** *hostname ip-address*
取消主机名和对应的 IP 地址	**undo ip host** *hostname* [*ip-address*]

缺省情况下，无主机名与主机 IP 地址对应。

5.2.6 配置静态路由

可以使用以下命令配置一条静态路由，用于通过网络对交换机进行访问。

请在系统视图下进行下列配置。

表5-7 配置静态路由

操作	命令
增加一条静态路由	**ip route-static** *ip-address* { *mask* | *mask-length* } { **null** *null-interface-number* | *gateway-address* } [**preference** *value*] [**reject** | **blackhole**]
删除一条静态路由	**undo ip route-static** *ip-address* { *mask* | *mask-length* } [**null** *null-interface-number* | *gateway-address*] [**preference** *value*] [**reject** | **blackhole**]

5.2.7 配置静态路由的缺省优先级

可以通过下列命令配置静态路由的缺省优先级。配置该命令改变缺省优先级的值后，随后配置的静态路由如果不指定其优先级，则其优先级为该命令配置的缺省优先级。

请在系统视图下进行下列配置。

表5-8 配置静态路由的缺省优先级

操作	命令
配置静态路由的缺省优先级	**ip route-static default-preference** *default-preference-value*
取消静态路由缺省优先级的配置	**undo ip route-static default-preference**

缺省情况下，*default-preference-value* 的值为 60。

5.3 系统 IP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后系统 IP 的运行情况，通过查看显示信息验证配置的效果。

表5-9 系统 IP 显示和调试

操作	命令
查看网络所有主机和对应的 IP 地址	**display ip host**
查看管理 VLAN 接口 IP 的相关信息	**display ip interface vlan-interface** *vlan-id*
查看管理 VLAN 接口的相关信息	**display interface vlan-interface** [*vlan_id*]
查看路由表摘要信息	**display ip routing-table**
查看路由表详细信息	**display ip routing-table verbose**
查看指定目的地址的路由	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]
查看指定目的地址范围内的路由	**display ip routing-table** *ip_address1 mask1 ip_address2 mask2* [**verbose**]

目 录

第1章 以太网端口配置

1.1 以太网端口简介

S5012G 以太网交换机提供 12 个 10/100/1000Base-T 自适应端口及 4 个 Combo GBIC（Gigabit interface convertor）端口，用户可根据自己的需要选配千兆光模块。

S5012T-12/10GBC 以太网交换机提供 10 个 GBIC 端口、2 个 10/100/1000Base-T 以太网端口及 2 个 Combo 10/100/1000Base-T 以太网端口，用户可根据自己的需要选配千兆光模块。

S5024G-24/20TP 以太网交换机提供 20 个 10/100/1000Base-T 以太网端口及 4 个 GBIC 端口，用户可根据自己的需要选配千兆光模块。

S5000 系列以太网交换机支持的以太网端口特性如下：

- 10/100/1000Base-T 以太网端口支持 MDI/MDI-X 自适应，工作方式为 1000M 全双工，100M 半双工/全双工或 10M 半双工/全双工。可以与其他网络设备协商确定工作方式和速率，自动选择最合适的工作方式和速率，从而大大简化系统的配置和管理。
- GBIC 端口工作在千兆全双工模式下，双工模式可以设置为 **full**（全双工）和 **auto**（自协商），速率可以设置为 **1000**（1000Mbit/s）和 **auto**（自协商）。
- Combo GBIC 端口的工作方式为 1000M 全双工，100M 半双工/全双工或 10M 半双工/全双工。

几种以太网端口的配置基本相同，下面一起介绍。

1.2 以太网端口配置

以太网端口配置包括：

- 进入以太网端口视图
- 打开/关闭以太网端口
- 对以太网端口进行描述
- 设置以太网端口双工状态
- 设置以太网端口速率

- 设置以太网端口流量控制
- 允许/禁止长帧通过以太网端口
- 设置以太网端口风暴抑制比
- 设置以太网端口的链路类型
- 把当前以太网端口加入到指定 VLAN
- 设置以太网端口缺省 VLAN ID
- 设置端口统计信息的时间间隔

1.2.1 进入以太网端口视图

要对以太网端口进行配置，首先要进入以太网端口视图。

请在系统视图下进行下列配置。

表1-1 进入以太网端口视图

操作	命令
进入以太网端口视图	**interface** { *interface_type interface_num* | *interface_name* }

1.2.2 打开/关闭以太网端口

当端口的相关参数及协议配置好之后，可以使用以下命令打开端口；如果想使某端口不再转发数据，可以使用以下命令关闭端口。

请在以太网端口视图下进行下列配置。

表1-2 打开或关闭以太网端口

操作	命令
关闭以太网端口	**shutdown**
打开以太网端口	**undo shutdown**

缺省情况下，端口为打开状态。

需要注意的是，100Base-TX 透明传输以太网端口不支持本操作。

1.2.3 对以太网端口进行描述

可以使用以下命令设置端口的描述字符串，以区分各个端口。

请在以太网端口视图下进行下列配置。

表1-3 对以太网端口进行描述

操作	命令
设置以太网端口描述字符串	**description** *text*
删除以太网端口描述字符串	**undo description**

缺省情况下，端口的描述字符串为空字符串。

1.2.4 设置以太网端口双工状态

当希望端口在发送数据包的同时可以接收数据包，可以将端口设置为全双工属性；当希望端口同一时刻只能发送数据包或接收数据包时，可以将端口设置为半双工属性；当设置端口为自协商状态时，端口的双工状态由本端口和对端端口自动协商而定。

请在以太网端口视图下进行下列配置。

表1-4 设置以太网端口双工状态

操作	命令
设置以太网端口的双工状态	**duplex** { **auto** | **full** | **half** }
恢复以太网端口的双工状态为缺省值	**undo duplex**

需要注意的是，10/100/1000Base-T 以太网端口及 Combo GBIC 端口可以工作在全双工、半双工或自协商模式下。但当速率设置为 1000Mbit/s 后，双工状态只可以设置为 **full**（全双工）或 **auto**（自协商）。GBIC 端口工作在全双工模式下，可以设置为 **full**（全双工）和 **auto**（自协商）。

缺省情况下，端口的双工状态为 **auto**（自协商）状态。

1.2.5 设置以太网端口速率

可以使用以下命令对以太网端口的速率进行设置，当设置端口速率为自协商状态时，端口的速率由本端口和对端端口双方自动协商而定。

请在以太网端口视图下进行下列设置。

表1-5 设置以太网端口速率

操作	命令
设置百兆以太网端口的速率	**speed { 10 | 100 | auto }**
设置千兆以太网端口的速率	**speed { 10 | 100 | 1000 | auto }**
恢复以太网端口的速率为缺省值	**undo speed**

需要注意的是，10/100/1000Base-T 以太网端口及 Combo GBIC 端口支持 10Mbit/s、100Mbit/s、1000Mbit/s 三种速率，可以根据需要选择合适的端口速率。但当双工状态设置为半双工模式后，就不能设置为 1000Mbit/s 速率。GBIC 端口支持 1000Mbit/s 速率，可以设置为 **1000**（1000Mbit/s）或 **auto**（自协商）。

缺省情况下，以太网端口的速率处于 **auto**（自协商）状态。

1.2.6 设置以太网端口流量控制

当本端和对端交换机都开启了流量控制功能后，如果本端交换机发生拥塞，它将向对端交换机发送消息，通知对端交换机暂时停止发送报文；而对端交换机在接收到该消息后将暂时停止向本端发送报文；反之亦然。从而避免了报文丢失现象的发生。可以使用以下命令对以太网端口是否开启流量控制功能进行设置。

请在以太网端口视图下进行下列配置。

表1-6 设置以太网端口流量控制

操作	命令
开启以太网端口的流量控制	**flow-control**
关闭以太网端口的流量控制	**undo flow-control**

缺省情况下，端口的流量控制为关闭状态。

1.2.7 允许/禁止长帧通过以太网端口

当以太网端口在进行文件传输等大吞吐量数据交换的时候，可能会遇到大于标准以太网帧长的长帧。可以通过以下的命令设置禁止长帧通过以太网端口或允许大于 1518 字节而小于 9216 字节的长帧通过以太网端口。

请在以太网端口视图下进行下列配置。

表1-7 允许/禁止长帧通过以太网端口

操作	命令
允许长帧通过以太网端口	**jumboframe enable**
禁止长帧通过以太网端口	**undo jumboframe enable**

缺省情况下，允许大于 1518 字节而小于 9216 字节的长帧通过以太网端口。

1.2.8 设置以太网端口风暴抑制比

可以使用以下的命令限制端口上允许通过的广播/组播/未知单播流量的大小，当广播/组播/未知单播流量超过用户设置的值后，系统将作丢弃处理，使广播/组播/未知单播所占的流量比例降低到合理的范围，从而有效地抑制广播/组播/未知单播风暴，避免网络拥塞，保证网络业务的正常运行。以端口最大的广播/组播/未知单播流量的线速度百分比作为参数，百分比越小，表示允许通过的广播/组播/未知单播流量越小；当百分比为 100 时，表示不对该端口进行风暴抑制。

请在以太网端口视图下进行下列配置。

表1-8 设置以太网端口风暴抑制比

操作	命令
设置以太网端口的广播风暴抑制比例	**broadcast-suppression** *pct*
恢复以太网端口的广播风暴抑制比例为缺省值	**undo broadcast-suppression**
设置以太网端口的组播风暴抑制比例	**multicast-suppression** *pct*
恢复以太网端口的组播风暴抑制比例为缺省值	**undo multicast-suppression**
设置以太网端口的未知单播风暴抑制比例	**unicast-suppression** *pct*
恢复以太网端口的未知单播风暴抑制比例为缺省值	**undo unicast-suppression**

缺省情况下，允许通过的广播/组播/未知单播流量为 100%，即不对广播/组播/未知单播流量进行抑制。

1.2.9 设置以太网端口的链路类型

以太网端口有三种链路类型：Access、Hybrid 和 Trunk。Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；Trunk 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接

的端口；Hybrid 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。Hybrid 端口和 Trunk 端口的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。

请在以太网端口视图下进行下列设置。

表1-9 设置以太网端口的链路类型

操作	命令
设置端口为 Access 端口	**port link-type access**
设置端口为 Hybrid 端口	**port link-type hybrid**
设置端口为 Trunk 端口	**port link-type trunk**
恢复端口的链路类型为缺省的 Access 端口	**undo port link-type**

三种类型的端口可以共存在一台以太网交换机上，但 Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再设置为其他类型端口。例如：Trunk 端口不能直接被设置为 Hybrid 端口，只能先设为 Access 端口，再设置为 Hybrid 端口。

缺省情况下，端口为 Access 端口。

1.2.10 把当前以太网端口加入到指定 VLAN

本配置任务把当前以太网端口加入到指定的 VLAN 中。Access 端口只能加入到 1 个 VLAN 中，Hybrid 端口和 Trunk 端口可以加入到多个 VLAN 中。

请在以太网端口视图下进行下列设置。

表1-10 把当前以太网端口加入到指定 VLAN

操作	命令
把当前 Access 端口加入到指定 VLAN	**port access vlan** *vlan_id*
将当前 Hybrid 端口加入到指定 VLAN	**port hybrid vlan** *vlan_id_list* { **tagged** | **untagged** }
把当前 Trunk 端口加入到指定 VLAN	**port trunk permit vlan** { *vlan_id_list* | **all** }
把当前 Access 端口从指定 VLAN 删除	**undo port access vlan**
把当前 Hybrid 端口从指定 VLAN 中删除	**undo port hybrid vlan** *vlan_id_list*
把当前 Trunk 端口从指定 VLAN 中删除	**undo port trunk permit vlan** { *vlan_id_list* | **all** }

需要注意的是：Access 端口加入的 VLAN 必须已经存在并且不能是 VLAN 1；Hybrid 端口加入的 VLAN 必须已经存在；Trunk 端口加入的 VLAN 不能是 VLAN 1。

执行了本配置，当前以太网端口就可以转发指定 VLAN 的报文。Hybrid 端口和 Trunk 端口可以加入到多个 VLAN 中，从而实现本交换机上的 VLAN 与对端交换机上相同 VLAN 的互通。Hybrid 端口还可以设置哪些 VLAN 的报文打上标签，哪些不打标签，为实现对不同 VLAN 报文执行不同处理流程打下基础。

1.2.11 设置以太网端口缺省 VLAN ID

Access 端口只属于 1 个 VLAN，所以它的缺省 VLAN 就是它所在的 VLAN，不用设置；Hybrid 端口和 Trunk 端口属于多个 VLAN，所以需要设置缺省 VLAN ID。如果设置了端口的缺省 VLAN ID，当端口接收到不带 VLAN Tag 的报文后，则将报文转发到属于缺省 VLAN 的端口；当端口发送带有 VLAN Tag 的报文时，如果该报文的 VLAN ID 与端口缺省的 VLAN ID 相同，则系统将去掉报文的 VLAN Tag，然后再发送该报文。

请在以太网端口视图下进行下列配置。

表1-11 设置以太网端口缺省 VLAN ID

操作	命令
设置 Hybrid 端口的缺省 VLAN ID	**port hybrid pvid vlan** *vlan_id*
设置 Trunk 端口的缺省 VLAN ID	**port trunk pvid vlan** *vlan_id*
恢复 Hybrid 端口的缺省 VLAN ID 为缺省值	**undo port hybrid pvid**
恢复 Trunk 端口的缺省 VLAN ID 为缺省值	**undo port trunk pvid**

需要注意的是，本 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 和相连的对端交换机的 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 必须一致，否则报文将不能正确传输。

缺省情况下，Hybrid 端口和 Trunk 端口的缺省 VLAN 为 VLAN 1，Access 端口的缺省 VLAN 是本身所属于的 VLAN。

1.2.12 设置端口统计信息的时间间隔

使用以下的配置任务可以设置端口统计信息的时间间隔，交换机在统计端口信息时统计的是此时间间隔内的平均速率。

请在以太网端口视图下进行下列配置。

表1-12 设置端口统计信息的时间间隔

操作	命令
设置端口统计信息的时间间隔	**flow-interval** *interval*
恢复端口统计信息的时间间隔为缺省值	**undo flow-interval**

缺省情况下，端口统计信息的时间间隔为 300 秒。

1.3 以太网端口显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后以太网端口的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除以太网端口的统计信息。

在以太网端口视图下，执行 **loopback** 命令进行环回测试，可以检验以太网端口是否正常工作，此时，端口将不能正确转发数据包，在执行一定时间后环回测试会自动结束。

表1-13 以太网端口显示和调试

操作	命令
设置以太网端口进行环回测试	**loopback** { **external** | **internal** }
显示端口的所有信息	**display interface** { *interface_type* | *interface_type interface_num* | *interface_name* }
显示 Hybrid 端口或 Trunk 端口	**display port** { **hybrid** | **trunk** }
清除以太网端口的统计信息	**reset counters interface** [*interface_type* | *interface_type interface_num* | *interface_name*]

需要注意的是，如果端口执行了 **shutdown** 命令后则不能进行 loopback 环回测试；在进行环回测试时系统将禁止在端口上进行 **speed**，**duplex**，**shutdown** 操作；有些端口不支持环回测试，在这些端口上进行环回测试时系统会给出提示。

1.4 以太网端口配置举例

1. 组网需求

以太网交换机 Switch A 与对端交换机 Switch B 使用 Trunk 端口 GigabitEthernet0/1 相连，本例将为该 Trunk 端口配置缺省的 VLAN ID，验证 **port trunk pvid vlan** 命令的使用。**port trunk pvid vlan** 的典型应用是当接收到没有标记的报文时，该 Trunk 端口将此报文发往缺省 VLAN ID 标识的 VLAN。

2. 组网图

图1-1 配置 Trunk 端口的缺省 VLAN ID 示例图

3. 配置步骤

以下只列出了 Switch A 的配置，Switch B 应作类似的配置：

进入 GigabitEthernet0/1 以太网端口视图。

[Quidway] interface gigabitethernet0/1

配置端口 GigabitEthernet0/1 为 Trunk 端口，并允许 2、6 到 50、100 等 VLAN 通过。

[Quidway-GigabitEthernet0/1] port link-type trunk

[Quidway-GigabitEthernet0/1] port trunk permit vlan 2 6 to 50 100

创建 VLAN 100。

[Quidway] vlan 100

配置端口 GigabitEthernet0/1 的缺省 VLAN ID 为 100。

[Quidway-GigabitEthernet0/1] port trunk pvid vlan 100

1.5 以太网端口排错

故障现象：配置缺省 VLAN ID 不成功。

故障排除：可以按照如下步骤进行。

- 使用 **display interface** 或 **display port** 命令检查该端口是否为 Trunk 端口或 Hybrid 端口。如不是，则应先将其配置成 Trunk 端口或 Hybrid 端口。
- 接着再配置缺省 VLAN ID。

第2章 以太网端口汇聚配置

2.1 以太网端口汇聚简介

端口汇聚是将多个端口聚合在一起形成 1 个汇聚组，以实现出/入负荷在各成员端口中的分担，同时也提供了更高的连接可靠性。

一台 S5012G 和 S5012T-12/10GBC 以太网交换机最多可以有 6 个汇聚组，1 个汇聚组最多可以有 8 个端口。组内的端口号必须连续，但对起始端口无特殊要求。

一台 S5024G-24/20TP 以太网交换机最多可以有 12 个汇聚组，1 个汇聚组最多可以有 8 个端口。组内的端口号必须连续，但对起始端口无特殊要求。

在一个端口汇聚组中，端口号最小的作为主端口，其他的作为成员端口。同一个汇聚组中成员端口的链路类型与主端口的链路类型保持一致，即如果主端口为 Trunk 端口，则成员端口也为 Trunk 端口；如主端口的链路类型改为 Access 端口，则成员端口的链路类型也变为 Access 端口。

2.2 以太网端口汇聚配置

以太网端口汇聚配置包括：

- 将一组以太网端口设置为汇聚端口

2.2.1 将一组以太网端口设置为汇聚端口

该配置任务用来设置或删除以太网的汇聚端口。

请在系统视图下进行下列配置。

表2-1 配置以太网端口汇聚

操作	命令
设置以太网汇聚端口	**link-aggregation** *interface_name1* **to** *interface_name2* { **both** | **ingress** }
删除以太网汇聚端口	**undo link-aggregation** { *master_interface_name* | **all** }

需要注意的是，进行汇聚的以太网端口的速率必须相同，且必须工作在全双工模式，否则无法实现汇聚。

2.3 以太网端口汇聚显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后以太网端口汇聚的运行情况，通过查看显示信息验证配置的效果。

表2-2 显示汇聚端口的信息

操作	命令
显示汇聚端口的信息	**display link-aggregation** [*master_interface_name*]

2.4 以太网端口汇聚配置举例

1. 组网需求

本例将验证端口聚合命令的使用，它将多个端口聚合在一起，以实现对出/入负荷在各成员端口中进行分担。端口聚合的典型应用是将多个 Trunk 端口聚合在一起，因为 Trunk 端口上允许多个 VLAN 通过，Trunk 端口上流量较大，需要将流量在各个端口中进行分担。

以太网交换机 Switch A 用 3 个端口聚合接入以太网交换机 Switch B，Switch A 的接入端口为 GigabitEthernet0/1～GigabitEthernet0/3。

2. 组网图

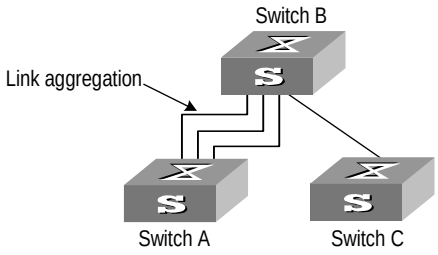


图2-1 配置聚合以太网端口示例图

3. 配置步骤

以下只列出了 Switch A 的配置，Switch B 上应作相应的配置，汇聚才能实际有效：

将以太网端口 GigabitEthernet0/1 至 GigabitEthernet0/3 聚合在一起。

[Quidway] link-aggregation gigabitethernet0/1 to gigabitethernet0/3 both

显示该汇聚端口的信息。

[Quidway] display link-aggregation gigabitethernet0/1

```
 Master port: GigabitEthernet0/1
Other sub-ports:
     GigabitEthernet0/2
     GigabitEthernet0/3
Mode: both
```

2.5 以太网端口汇聚配置排错

故障现象：当配置端口汇聚时，出现配置不成功的提示信息。

故障排除：

- 检查输入的起始端口是否小于结束端口，如是则转下一步。
- 检查所配置的端口是否属于其他已存在的汇聚组，如否则转下一步。
- 检查所汇聚的端口的速率是否相同且工作在全双工模式，如是，则转下一步。
- 检查汇聚组中的端口总数目是否小于或等于 8 个。
- 如果正确后，再转而配置该端口汇聚。

目 录

第1章 VLAN 配置

1.1 VLAN 简介

VLAN（Virtual Local Area Network），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虚拟工作组的技术。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案。

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域（或称虚拟 LAN，即 VLAN），每一个 VLAN 都包含一组有着相同需求的计算机，由于 VLAN 是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个计算机无须被放置在同一个物理空间里，即这些计算机不一定属于同一个物理 LAN 网段。

VLAN 的优势在于 VLAN 内部的广播和单播流量不会被转发到其它 VLAN 中，从而有助于控制网络流量、减少设备投资、简化网络管理、提高网络安全性。

1.2 VLAN 配置

对 VLAN 进行配置时，首先应根据需求创建 VLAN。

VLAN 配置包括：

- 创建/删除 VLAN
- 为 VLAN 指定以太网端口
- 为 VLAN 指定描述字符

1.2.1 创建/删除 VLAN

可以使用下面的命令来创建/删除 VLAN。创建 VLAN 时，如果该 VLAN 已存在，则直接进入该 VLAN 视图；如果该 VLAN 不存在，则此配置任务将首先创建 VLAN，然后进入 VLAN 视图。

请在系统视图下进行下列配置。

表1-1 创建/删除 VLAN

操作	命令
创建 VLAN 并进入 VLAN 视图	**vlan** *vlan_id*
删除已创建的 VLAN	**undo vlan** { *vlan_id* [**to** *vlan_id*] | **all** }

需要注意的是，缺省 VLAN 即 VLAN 1 不能被删除。

1.2.2 为 VLAN 指定以太网端口

可以使用下面的命令为 VLAN 指定以太网端口。

请在 VLAN 视图下进行下列配置。

表1-2 为 VLAN 指定端口

操作	命令
为指定的 VLAN 增加以太网端口	**port** *interface_list*
删除指定的 VLAN 的某些以太网端口	**undo port** *interface_list*

缺省情况下，系统将所有端口都加入到一个缺省的 VLAN 中，该 VLAN 的 ID 为 1。

需要注意的是，Trunk 和 Hybrid 端口只能通过以太网端口视图下的 **port** 和 **undo port** 命令加入 VLAN 或从 VLAN 中删除，而不能通过本命令实现。

1.2.3 为 VLAN 指定描述字符

可以使用下面的命令来指定 VLAN 的描述字符。

请在 VLAN 视图下进行下列配置。

表1-3 为 VLAN 指定描述字符

操作	命令
为 VLAN 指定一个描述字符串	**description** *string*
恢复 VLAN 的描述字符串为缺省描述	**undo description**

缺省情况下，VLAN 缺省描述字符串为该 VLAN 的 VLAN ID，例如“VLAN 0001”。

1.3 VLAN 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 VLAN 的运行情况，通过查看显示信息验证配置的效果。

表1-4 VLAN 的显示和调试

操作	命令
显示 VLAN 相关信息	**display vlan** [*vlan_id* | **all** | **static** | **dynamic**]

1.4 VLAN 典型配置举例

1. 组网需求

现有 VLAN2、VLAN3，通过配置将端口 GigabitEthernet0/1 和 GigabitEthernet0/2 包含到 VLAN2 中，将端口 GigabitEthernet0/3 和 GigabitEthernet0/4 包含到 VLAN3 中。

2. 组网图

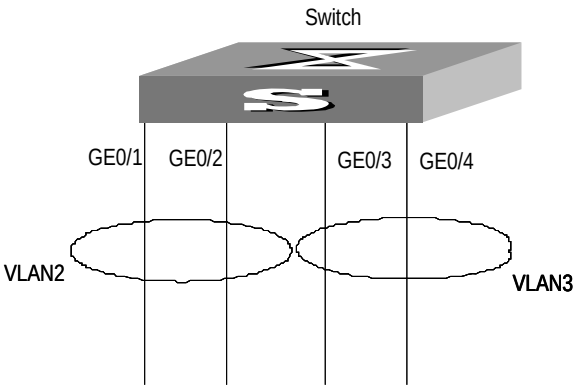


图1-1 VLAN 配置示例图

3. 配置步骤

创建 VLAN2 并进入其视图。

[Quidway] vlan 2

向 VLAN2 中加入端口 GigabitEthernet0/1 和 GigabitEthernet0/2。

[Quidway-vlan2] port gigabitethernet0/1 gigabitethernet0/2

创建 VLAN3 并进入其视图。

[Quidway-vlan2] vlan 3

向 VLAN3 中加入端口 GigabitEthernet0/3 和 GigabitEthernet0/4。

[Quidway-vlan3] port gigabitethernet0/3 gigabitethernet0/4

第2章 GARP/GVRP 配置

2.1 GARP 配置

2.1.1 GARP 协议简介

GARP（Generic Attribute Registration Protocol）是一种通用的属性注册协议，该协议提供了一种机制用于协助同一个交换网内的交换成员之间分发、传播和注册某种信息（如 VLAN、组播地址等）。

GARP 本身不作为一个实体存在于交换机中，遵循 GARP 协议的应用实体称为 GARP 应用，目前主要的 GARP 应用为 GVRP 和 GMRP。其中，GVRP 的详细介绍请参见本章中“GVRP 配置”一节的介绍，GMRP 将在“组播配置”部分介绍。当 GARP 应用实体存在于交换机的某个端口上时，该端口对应于一个 GARP 应用实体。

通过 GARP 机制，一个 GARP 成员上的配置信息会迅速传播到整个交换网。GARP 成员可以是终端工作站或网桥。GARP 成员通过声明或回收声明通知其它的 GARP 成员注册或注销自己的属性信息，并根据其它 GARP 成员的声明或回收声明注册或注销对方的属性信息。

GARP 成员之间的信息交换借助于消息完成，GARP 起主要作用的消息类型有三类，分别为 Join、Leave 和 LeaveAll。当一个 GARP 应用实体希望其它交换机注册自己的某属性信息时，将对外发送 Join 消息。当一个 GARP 应用实体希望其它交换机注销自己的某属性信息时，将对外发送 Leave 消息。每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当超时后将对外发送 LeaveAll 消息。Join 消息与 Leave 消息配合确保消息的注销或重新注册。通过消息交互，所有待注册的属性信息可以传播到同一交换网的所有交换机上。

GARP 应用实体的协议数据报文的目的 MAC 地址都是特定的组播 MAC 地址。支持 GARP 特性的交换机在接收到 GARP 应用实体的报文后，会根据其目的 MAC 地址加以区分并交给不同的 GARP 应用（如 GVRP 或 GMRP）去处理。

GARP（以及 GMRP）在 IEEE 802.1p 标准（现已合入 IEEE 802.1D 标准）文本中有详细的表述。Quidway 系列交换机对符合 IEEE 标准的 GARP 提供完备的支持。

GARP 配置包括：

- 配置 GARP 定时器参数

📖 **说明：**

(1) GARP 定时器的值将应用于所有在同一交换网内运行的 GARP 应用，包括 GVRP 和 GMRP。

(2) 在同一交换网内的所有交换设备的 GARP 定时器必须设置为相同的值，否则 GARP 应用将不能正常工作。

2.1.2 配置 GARP 定时器参数

GARP 的定时器包括 Hold 定时器、Join 定时器、Leave 定时器和 LeaveAll 定时器。

GARP 应用实体在 Join 定时器超时后将对外发送 Join 消息，以使其它 GARP 应用实体注册自己的信息。

当一个 GARP 应用实体希望注销某属性信息时，将对外发送 Leave 消息，接收到该消息的 GARP 应用实体启动 Leave 定时器，如果在该定时器超时之前没有再次收到 Join 消息，则注销该属性信息。

每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

当 GARP 应用实体接收到某注册信息时，不立即对外发送 Join 消息，而是启动 Hold 定时器，当该定时器超时后，再对外发送 Join 消息，以便在 Hold 定时器时间内收到的所有注册信息可以放在同一帧中发送，从而节省带宽资源。

请在以太网端口视图下配置 Hold 定时器、Join 定时器和 Leave 定时器；在系统视图下配置 LeaveAll 定时器。

表2-1 配置 GARP 定时器

操作	命令
配置 GARP 的 Hold 定时器、Join 定时器和 Leave 定时器	**garp timer** { **hold** | **join** | **leave** } *timer_value*
配置 GARP 的 LeaveAll 定时器	**garp timer leaveall** *timer_value*
将 GARP 的 Hold 定时器、Join 定时器和 Leave 定时器恢复为缺省值	**undo garp timer** { **hold** | **join** | **leave** }
将 GARP 的 LeaveAll 定时器恢复为缺省值	**undo garp timer leaveall**

需要注意的是，Join 定时器的值应大于等于 2 倍 Hold 定时器的值；Leave 定时器的值应大于 2 倍 Join 定时器的值并小于 LeaveAll 定时器的值，否则系统会报错。

缺省情况下，Hold 定时器为 10 厘秒，Join 定时器为 20 厘秒，Leave 定时器为 60 厘秒，LeaveAll 定时器为 1000 厘秒。

2.1.3 GARP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 GARP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可清除 GARP 相关配置；执行 **debugging** 命令可对 GARP 进行调试。

表2-2 GARP 的显示和调试

操作	命令
显示 GARP 的统计信息	**display garp statistics** [**interface** *interface-list*]
显示 GARP 定时器参数	**display garp timer** [**interface** *interface-list*]
清除 GARP 统计信息	**reset garp statistics** [**interface** *interface-list*]
开启 GARP 的事件调试开关	**debugging garp event**
关闭 GARP 的事件调试开关	**undo debugging garp event**

2.2 GVRP 配置

2.2.1 GVRP 协议简介

GVRP（GARP VLAN Registration Protocol）是 GARP 的一种应用，它基于 GARP 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的交换机中。所有支持 GVRP 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，包括当前的 VLAN 成员、这些 VLAN 成员可以通过哪个端口到达等。而且所有支持 GVRP 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 GVRP 特性的设备的 VLAN 信息达成一致。GVRP 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。

GVRP 在 IEEE 802.1Q 标准文本中有详细的表述。Quidway 系列交换机对符合 IEEE 标准的 GVRP 提供完备的支持。

GVRP 配置包括：

- 全局开启/关闭 GVRP
- 端口开启/关闭 GVRP
- 配置 GVRP 注册类型

在上述各项配置任务中，必须先启动全局 GVRP，才能开启端口 GVRP；而 GVRP 注册类型在启动了端口 GVRP 以后才能生效。此外，GVRP 必须在 Trunk 端口上进行设置。

2.2.2 全局开启/关闭 GVRP

可以使用下面的命令配置全局开启/关闭 GVRP。

请在系统视图下进行下列配置。

表2-3 全局开启/关闭 GVRP

操作	命令
全局开启 GVRP	**gvrp**
将全局 GVRP 恢复为缺省关闭状态	**undo gvrp**

缺省情况下，全局 GVRP 处于关闭状态。

2.2.3 端口开启/关闭 GVRP

可以使用下面的命令配置端口开启/关闭 GVRP。

请在以太网端口视图下进行下列配置。

表2-4 端口开启/关闭 GVRP

操作	命令
开启端口 GVRP	**gvrp**
将端口 GVRP 恢复为缺省关闭状态	**undo gvrp**

需要注意的是，在开启端口 GVRP 之前，必须先开启全局 GVRP，并且开启/关闭端口 GVRP 必须在 Trunk 端口操作。

缺省情况下，端口 GVRP 处于关闭状态。

2.2.4 配置 GVRP 注册类型

GVRP 的注册类型包括：Normal、Fixed 和 Forbidden（请参考 IEEE 802.1Q）。

- 当一个端口被配置为 Normal 注册模式时，允许在该端口动态或手工创建、注册和注销 VLAN。
- 当把一个 Trunk 端口设置为 fixed 模式时，如果在交换机上创建一个静态 VLAN 且该 Trunk 端口允许这个 VLAN 通过，系统就会将这个端口加入到这个 VLAN 中，同时 GVRP 会在本地 GVRP 数据库中（GVRP 维护的一个链表）添加这个 VLAN 的表项。但是 GVRP 不能通过这个端口学习动态 VLAN，同时从本交换机其它端口学习到的动态 VLAN 也不能从这个端口向外发送相关的声明。
- 当一个端口被配置为 Forbidden 注册模式时，在该端口将注销除 VLAN1 之外的所有 VLAN，并且禁止在该端口创建和注册任何其它 VLAN。

请在以太网端口视图下进行下列配置。

表2-5 配置 GVRP 注册类型

操作	命令
配置 GVRP 注册类型	**gvrp registration** { **normal** | **fixed** | **forbidden** }
将 GVRP 注册类型恢复为缺省值	**undo gvrp registration**

缺省情况下，GVRP 注册类型为 Normal。

2.2.5 GVRP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 GVRP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可对 GVRP 进行调试。

表2-6 GVRP 的显示和调试

操作	命令
显示 GVRP 统计信息	**display gvrp statistics** [**interface** *interface-list*]
显示 GVRP 全局状态信息	**display gvrp status**
开启 GVRP 的数据包或事件调试开关	**debugging gvrp** { **packet** | **event**}
关闭 GVRP 的数据包或事件调试开关	**undo debugging gvrp** { **packet** | **event**}

2.2.6 GVRP 典型配置举例

1. 组网需求

为了实现交换机之间 VLAN 信息的动态注册和更新，需要在交换机上启动 GVRP。

2. 组网图

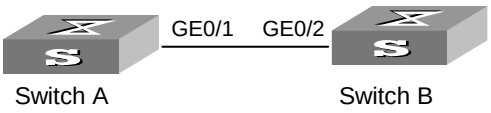


图2-1 GVRP 配置示例图

3. 配置步骤

配置 Switch A：

开启全局 GVRP。

[Quidway] gvrp

将以太网端口 GigabitEthernet0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

[Quidway] interface gigabitethernet0/1

[Quidway-GigabitEthernet0/1] port link-type trunk

[Quidway-GigabitEthernet0/1] port trunk permit vlan all

在 Trunk 端口上开启 GVRP。

[Quidway-GigabitEthernet0/1］gvrp

配置 Switch B：

开启全局 GVRP。

[Quidway] gvrp

将以太网端口 GigabitEthernet0/2 配置为 Trunk 端口，并允许所有 VLAN 通过。

[Quidway] interface gigabitethernet0/2

[Quidway-GigabitEthernet0/2］port link-type trunk

[Quidway-GigabitEthernet0/2］port trunk permit vlan all

在 Trunk 端口上开启 GVRP。

[Quidway-GigabitEthernet0/2］gvrp

目 录

第1章 GMRP 配置

1.1 GMRP 协议简介

GMRP（GARP Multicast Registration Protocol）是基于 GARP 的一个组播注册协议，用于维护交换机中的动态组播注册信息。所有支持 GMRP 的交换机都能够接收来自其他交换机的组播注册信息，并动态更新本地的组播注册信息，同时也能将本地的组播注册信息向其他交换机传播。这种信息交换机制，确保了同一交换网内所有支持 GMRP 的设备维护的组播信息的一致性。

当一台主机想要加入一个某个组播组时，它将发出 GMRP 加入消息。交换机将接到 GMRP 加入消息的端口加入到该组播组中，并在 VLAN 中广播该 GMRP 加入消息，VLAN 中的组播源就可以知晓组播成员的存在。当组播源向组播组发送组播报文时，交换机就只把组播报文转发给与该组播组成员相连的端口，从而实现了在 VLAN 内的二层组播。

GMRP 传播的组播注册信息既包括本地手工配置的静态组播注册信息，也包括由其他交换机动态注册到本地交换机的组播注册信息。

1.2 GMRP 配置

GMRP 主要配置包括：

- 开启/关闭全局 GMRP
- 开启/关闭端口 GMRP

在配置任务中，必须先开启全局 GMRP，才能开启端口 GMRP。

1.2.1 开启/关闭全局 GMRP

请在系统视图下进行下列配置。

表1-1 开启/关闭全局 GMRP

操作	命令
开启全局 GMRP	**gmrp**
关闭全局 GMRP	**undo gmrp**

缺省情况下，不启动 GMRP。

1.2.2 开启/关闭端口 GMRP

请在以太网端口视图下进行下列配置。

表1-2 开启/关闭端口 GMRP

操作	命令
开启端口 GMRP	**gmrp**
关闭端口 GMRP	**undo gmrp**

在开启端口 GMRP 之前，必须先开启全局 GMRP。

缺省情况下，不启动端口 GMRP。

1.3 GMRP 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 GMRP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **debugging** 命令对 GMRP 进行调试。

表1-3 GMRP 显示和调试

操作	命令
显示 GMRP 统计信息	**display gmrp statistics** [**interface** *interface_list*]
显示 GMRP 全局状态信息	**display gmrp status**
打开 GMRP 调试开关	**debugging gmrp event**
关闭 GMRP 调试开关	**undo debugging gmrp event**

1.4 GMRP 典型配置举例

1. 组网需求

在交换机之间动态注册和更新组播信息。

2. 组网图

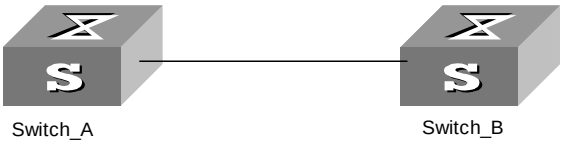


图1-1 GMRP 示例组网图

3. 配置步骤

配置 Switch_A：

启动全局 GMRP。

[Quidway] gmrp

启动端口 GMRP。

[Quidway] interface GigabitEthernet 0/1

[Quidway-GigabitEthernet0/1] gmrp

配置 Switch_B：

启动全局 GMRP。

[Quidway] gmrp

启动端口 GMRP。

[Quidway] interface GigabitEthernet 0/1

[Quidway-GigabitEthernet0/1] gmrp

第2章 IGMP Snooping 配置

2.1 IGMP Snooping 协议简介

2.1.1 IGMP Snooping 原理

IGMP Snooping（Internet Group Management Protocol Snooping）是运行在二层以太网交换机上的组播约束机制，用于管理和控制组播组。

IGMP Snooping 运行在链路层。当二层以太网交换机收到主机和路由器之间传递的 IGMP 报文时，IGMP Snooping 分析 IGMP 报文所带的信息。当监听到主机发出的 IGMP 主机报告报文（IGMP host report message）时，交换机就将与该主机加入到相应的组播表中；当监听到主机发出的 IGMP 离开报文（IGMP leave message）时，交换机就将删除与该主机对应的组播表项。通过不断地监控 IGMP 报文，交换机就可以在二层建立和维护 MAC 组播地址表。之后，交换机就可以根据 MAC 组播地址表进行转发从路由器下发的组播报文。

没有运行 IGMP Snooping 时，组播报文将在二层广播。如下图所示：

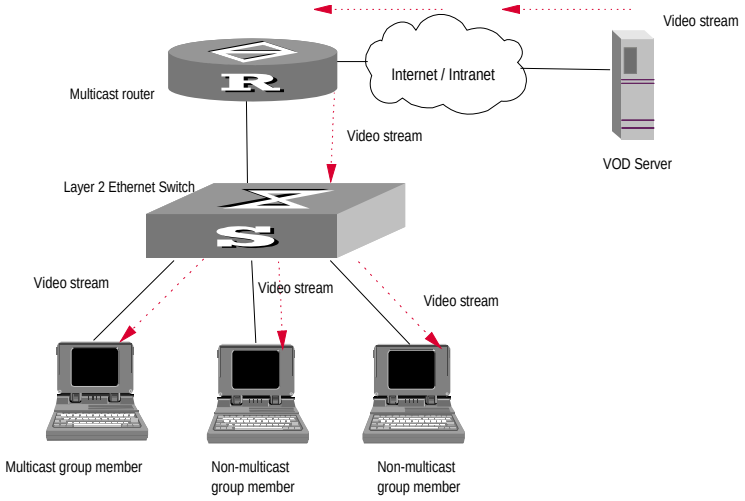


图2-1 没有 IGMP Snooping 时组播报文传播过程

运行 IGMP Snooping 后,报文将不再在二层广播，而是进行二层组播。如下图所示：

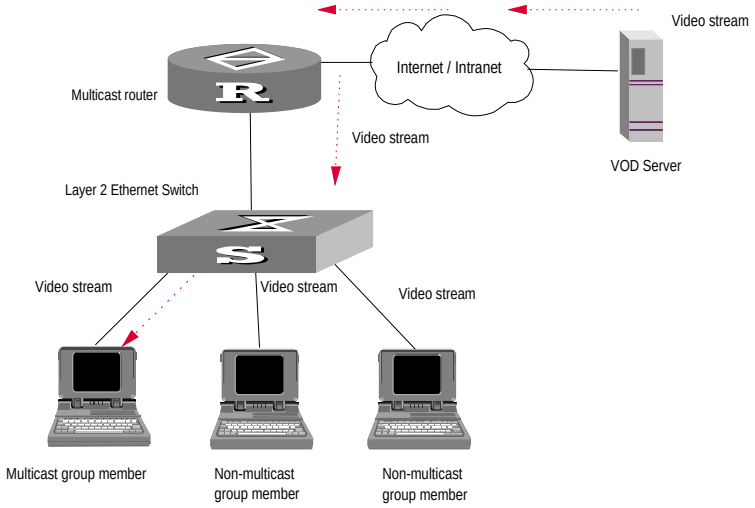


图2-2 实现 IGMP Snooping 时组播报文传播过程

2.1.2 IGMP Snooping 的实现

1. 与 IGMP Snooping 相关的概念

为描述方便，先介绍一下以太网交换机上与 IGMP Snooping 相关的概念：

- 路由器端口（Router Port）：以太网交换机上直接和组播路由器相连的端口。
- 组播成员端口：与组播组成员相连的端口。组播组成员此处是加入某个组播组的主机。
- MAC 组播组：以太网交换机维护的以 MAC 组播地址标识的组播组。
- 路由器端口老化时间：路由器端口老化定时器设置的时间，如果在此定时器超时的时候还没有收到 IGMP 通用查询报文，交换机就认为这个端口不再是一个路由器端口。
- 组播组成员端口老化时间：当一个端口加入到 IP 组播组中的时候会同时启动该端口的老化定时器，组播组端口成员老化时间就是该定时器设置的时间。如果在此定时器超时的时候还没有收到 IGMP 报告报文，以太网交换机则向该端口发送 IGMP 特定组查询报文。
- 最大响应查询时间：当向组播成员端口发送 IGMP 特定组查询报文的同时，以太网交换机会启动一个响应查询定时器，最大响应查询时间就是该定时器设置的时间。如果在最大响应查询时间之内没有收到 IGMP 报告报文，以太网交换机就把该端口从组播成员端口中删去。

2. 利用 IGMP Snooping 实现二层组播

以太网交换机通过运行 IGMP Snooping 实现对 IGMP 报文的侦测，并为主机及其对应端口与相应的组播组地址建立映射关系。为实现 IGMP Snooping，二层以太网交换机对各种 IGMP 报文的处理过程如下：

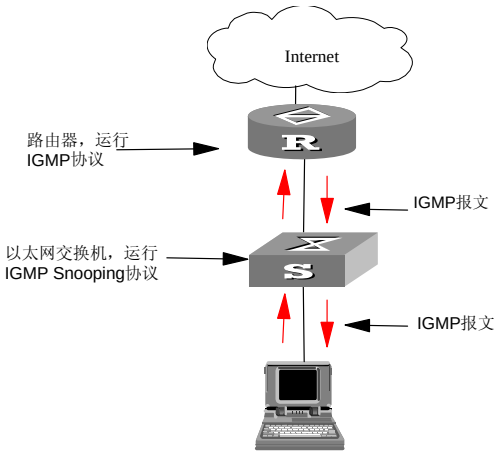


图2-3 实现 IGMP Snooping 示意图

- IGMP 通用查询报文：IGMP 通用查询报文是组播路由器向组播组成员发送的报文，用于查询哪些组播组存在成员。当收到 IGMP 通用查询报文时，如果收到通用查询报文的端口原来就是路由器端口，以太网交换机就重置该路由器端口的老化定时器；如果收到通用查询报文的端口原来不是路由器端口，则交换机通知组播路由器有成员需要加入某个组播组，同时启动对该路由器端口的老化定时器。
- IGMP 特定组查询报文：IGMP 特定组查询报文是组播路由器向组播组成员发送的报文，用于查询特定组播组是否存在成员。当以太网交换机收到 IGMP 特定组查询报文时，只向被查询的 IP 组播组发特定组查询。
- IGMP 报告报文：IGMP 报告报文是主机向组播路由器发送的报告报文，用于申请加入某个组播组或者应答 IGMP 查询报文。当以太网交换机收到 IGMP 报告报文时，首先判断该报文要加入的 IP 组播组对应的 MAC 组播组是否已经存在。如果对应的 MAC 组播组不存在，只是通知路由器有成员加入某个组播组，则会新建 MAC 组播组，将接收报告报文的端口加入该 MAC 组播组中，并启动该端口的老化定时器，然后将该端口所属 VLAN 下存在的所有路由器端口加入到此 MAC 组播转发表中，同时新建 IP 组播组，并将接收报告报文的端口加入到 IP 组播组中；如果该报文对应的 MAC 组播组已经存在，但是接收报告报文的端口不在该 MAC 组播组中，则将接收报告报文的端口加入 MAC 组播组中并启动

该端口的老化定时器，然后判断此报文对应的 IP 组播组是否存在：如果不存在，则新建 IP 组播组并把接收报告报文的端口加入到 IP 组播组中，如果存在则将接收报告报文的端口加入到 IP 组播组中；如果该报文对应的 MAC 组播组已存在，并且接收报告报文的端口也已经存在于该 MAC 组播组，则仅重置接收报告报文的端口上的老化定时器。

- IGMP 离开报文：IGMP 离开报文是组播组成员向组播路由器发送的报文，用于告知路由器主机离开了某个组播组。当以太网交换机收到对某 IP 组播组的离开报文，则会向接收此离开报文的端口发送所离开组的特定组查询报文，以确认此端口相连的主机中还有没有此组播组的其他成员，同时启动一个响应查询定时器。如果在该定时器超时的时候还没有收到该组播组的报告报文，则将该端口从相应 MAC 组播组中删去。如果 MAC 组播组没有组播成员端口时，交换机将通知组播路由器将该分支从组播树中删除。

2.2 IGMP Snooping 配置

IGMP Snooping 配置包括：

- 启动/关闭 IGMP Snooping
- 配置路由器端口老化时间
- 配置最大响应查询时间
- 配置组播组端口成员老化时间

在上述的配置任务中，启动 IGMP Snooping 是必须的，其余则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.2.1 启动/关闭 IGMP Snooping

为了控制 IGMP Snooping 是否在二层建立和维护 MAC 组播转发表，可以使用下面的命令来启动/关闭 IGMP Snooping。

请在系统视图下进行下列配置。

表2-1 启动/关闭 IGMP Snooping

操作	命令
启动/关闭 IGMP Snooping	**igmp-snooping** { **enable** | **disable** }
恢复 IGMP Snooping 为缺省状态	**undo igmp-snooping**

IGMP Snooping 和 GMRP 不能同时运行，可以在启动 IGMP Snooping 之前在所有视图下使用命令 **display gmrp status** 查看 GMRP 是否正在运行。此外，IGMP Snooping 和 IGMP 也不能同时在一台以太网交换机上运行。

缺省情况下，关闭 IGMP Snooping。

2.2.2 配置路由器端口老化时间

本配置任务用来手工设置路由器端口老化时间。如果在路由器端口老化时间之内没有收到路由器的通用查询报文，则把该路由器端口从所有的 MAC 组播组的端口成员中删去。

请在系统视图下进行下列配置。

表2-2 配置端口老化时间

操作	命令
配置端口老化时间	**igmp-snooping router-aging-time** *seconds*
恢复端口老化时间缺省值	**undo igmp-snooping router-aging-time**

缺省情况下，端口老化时间为 260 秒。

2.2.3 配置最大响应查询时间

本配置任务用来手工设置最大响应查询时间。如果在最大响应查询时间之内没有收到报告报文，以太网交换机就把该端口从组播组端口成员中删去。

请在系统视图下进行下列配置。

表2-3 配置最大响应查询时间

操作	命令
配置最大响应查询时间	**igmp-snooping max-response-time** *seconds*
恢复最大响应查询时间的缺省值	**undo Igmp-snooping max-response-time**

缺省情况下，响应查询的最晚时间为 10 秒。

2.2.4 配置组播组成员端口老化时间

本配置任务用来手工设置组播组成员端口老化时间。在成员端口老化时间之内，如果没有收到组播组报告报文，则向该端口发指定组查询，同时启动该 IP 组播组的响应查询定时器。

请在系统视图下进行下列配置。

表2-4 配置组播组成员老化时间

操作	命令
配置组播组成员老化时间	**igmp-snooping host-aging-time** *seconds*
恢复组播组成员老化时间的缺省值	**undo igmp-snooping host-aging-time**

缺省情况下，组播组成员端口老化时间为 260 秒。

2.3 IGMP Snooping 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 IGMP Snooping 的运行情况，通过查看显示信息验证配置的效果。

表2-5 IGMP Snooping 的显示和调试

操作	命令
显示当前 IGMP Snooping 的配置信息	**display igmp-snooping configuration**
显示 IGMP Snooping 对收发包的统计信息	**display igmp-snooping statistics**
显示 VLAN 下的 IP 组播组和 MAC 组播组信息	**display igmp-snooping group** [**vlan** *vlanid*]

2.4 IGMP Snooping 典型配置举例

2.4.1 启动 IGMP Snooping

1. 组网需求

为了实现交换机的 IGMP Snooping 功能，需要在交换机上启动 IGMP Snooping。交换机上的路由器端口接到路由器上，其他非路由器端口则接到用户的 PC 机上。

2. 组网图

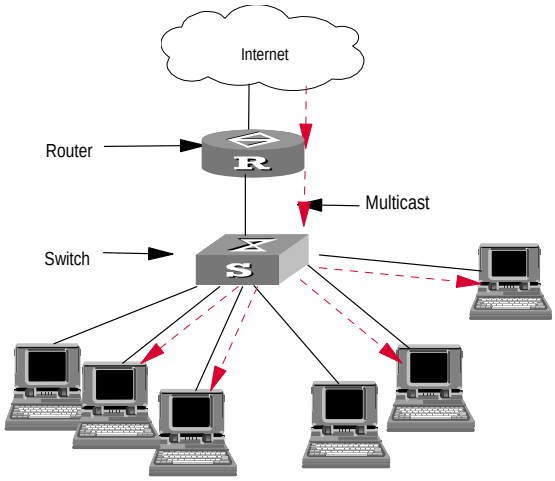


图2-4 配置 IGMP Snooping 组网图

3. 配置步骤

显示 GMRP 的状态。

<Quidway> display gmrp status

当 GMRP 没有运行时，查看 IGMP Snooping 当前的状态。

<Quidway> display igmp-snooping configuration

当 IGMP Snooping 没有启动时，启动 IGMP Snooping。

[Quidway] igmp-snooping enable

2.5 IGMP Snooping 故障诊断与排错

故障现象：交换机不能实现组播功能。

故障排除：

(1) IGMP Snooping 没有启动。

- 输入命令 **display current-configuration** 查看 IGMP Snooping 的状态。
- 如果 IGMP Snooping 没有启动，则在系统视图下输入命令 **igmp-snooping enable** 命令启动 IGMP Snooping。

(2) IGMP Snooping 建立的组播转发表不对。

- 输入命令：**display igmp-snooping group** 查看组播组是否是所预期的。
- 如果 IGMP Snooping 建立的组播组不正确，则向专业维护人员求助。

- 如果排除了原因 2，则进入原因分析 3。

(3) 底层建立的组播转发表不对。

- 在所有视图下使用命令 **display mac-address vlan** 显示底层在 *vlanid* 下所建立的 MAC 组播转发表是否和 IGMP Snooping 建立的 MAC 组播转发表一致。
- 如果不一致则请向维护人员求助。

第3章 未知组播丢弃特性配置

3.1 未知组播丢弃特性配置简介

通常情况下，如果交换机收到的组播数据报文的组播地址没有在本机注册，该报文会在 VLAN 内广播，而启动未知组播丢弃特性后，交换机收到未注册组播地址的组播数据报文，将丢弃该报文，从而节省了带宽，并提高系统的处理效率。

3.2 未知组播丢弃特性配置

未知组播丢弃特性的配置包括：

- 启动未知组播报文丢弃特性

3.2.1 启动未知组播报文丢弃特性

该特性启动后，交换机将丢弃未注册组播地址的数据报文。

请在系统视图下进行下列配置。

表3-1 启动/关闭未知组播报文丢弃特性

操作	命令
启动未知组播报文丢弃特性	**unknown-multicast drop enable**
关闭未知组播报文丢弃特性	**undo unknown-multicast drop enable**

缺省情况下，未注册组播地址的数据报文将在 VLAN 内广播。

目 录

第1章 ACL 配置

1.1 访问控制列表简介

1.1.1 访问控制列表概述

为了过滤通过网络设备的数据包，需要配置一系列的匹配规则，以识别需要过滤的对象。在识别出特定的对象之后，网络设备才能根据预先设定的策略允许或禁止相应的数据包通过。访问控制列表（Access Control List，ACL）就是用来实现这些功能。

ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。ACL 应用在交换机全局或端口，交换机根据 ACL 中指定的条件来检测数据包，从而决定是转发还是丢弃该数据包。

由 ACL 定义的数据包匹配规则，还可以在其它需要对流量进行区分的场合引用，如定义 QoS 中的流分类规则时。

一条访问控制规则可以由多条子规则组成。由于每一条子规则指定的数据包的范围大小有别，在匹配一个访问控制规则的时候就存在匹配顺序的问题。

1. ACL 直接下发到硬件中的情况

交换机中 ACL 可以直接下发到交换机的硬件中用于数据转发过程中的过滤和流分类。此时一条 ACL 中多个子规则的匹配顺序是由交换机的硬件决定的，用户即使在定义 ACL 时配置了匹配顺序也不起作用。

ACL 直接下发到硬件的情况包括：交换机实现 QoS 功能时引用 ACL、硬件转发时通过 ACL 过滤转发数据等。

2. ACL 被上层模块引用的情况

交换机也使用 ACL 来对由软件处理的报文进行过滤和流分类。此时 ACL 子规则的匹配顺序有两种：**config**（指定匹配该规则时按用户的配置顺序）和 **auto**（指定匹配该规则时系统自动排序，即按“深度优先”的顺序）。这种情况下用户可以在定义 ACL 的时候指定一条 ACL 中多个子规则的匹配顺序。用户一旦指定某一条访问控制列表的匹配顺序，就不能再更改该顺序。只有把该列表中所有的规则全部删除后，才能重新指定其匹配顺序。

ACL 被软件引用的情况包括：路由策略引用 ACL、对登录用户进行控制时引用 ACL 等。

📖 **说明：**

“深度优先”的原则是指：把指定数据包范围最小的语句排在最前面。这一点可以通过比较地址的通配符来实现，通配符越小，则指定的主机的范围就越小。比如 129.102.1.1 0.0.0.0 指定了一台主机: 129.102.1.1，而 129.102.1.1 0.0.255.255 则指定了一个网段：129.102.1.1～129.102.255.255。显然前者在访问控制规则中排在前面。具体标准为：对于基本访问控制规则的语句，直接比较源地址通配符，通配符相同的则按配置顺序；对于基于接口过滤的访问控制规则，配置了“**any**”的规则排在后面，其它按配置顺序；对于高级访问控制规则，首先比较源地址通配符，相同的再比较目的地址通配符，仍相同的则比较端口号的范围，范围小的排在前面，如果端口号范围也相同则按配置顺序。

1.1.2 以太网交换机支持的访问控制列表

在以太网交换机中，访问控制列表分为以下几类：

- 基于数字标识的基本访问控制列表。
- 基于名字标识的基本访问控制列表。
- 基于数字标识的高级访问控制列表。
- 基于名字标识的高级访问控制列表。
- 基于数字标识的二层访问控制列表。
- 基于名字标识的二层访问控制列表。

交换机上对各种访问控制列表的数目限制如下表所示：

表1-1 访问控制列表的数量限制

项目	数字取值范围
基于数字标识的基本访问控制列表	2000～2999
基于数字标识的高级访问控制列表	3000～3999
基于数字标识的二层访问控制列表	4000～4999
基于名字标识的基本访问控制列表	—
基于名字标识的高级访问控制列表	—
基于名字标识的二层访问控制列表	—

项目	数字取值范围
一条访问控制列表可以定义的子规则	0～127
交换机最多可以定义的子规则（所有访问控制列表的子规则之和）	—

📖 **说明：**

S5000 系列以太网交换机不支持配置用户自定义类型的访问控制列表，在命令行的提示中虽然有此类访问控制列表的描述，但是用户自定义类型的访问控制列表不能下发到硬件，也不能用于在各种 QoS 功能的应用中生效。

1.2 ACL 配置

访问控制列表配置包括：

- 配置时间段
- 定义访问控制列表
- 激活访问控制列表

以上三个步骤最好依次进行，先配置时间段，然后定义访问控制列表（在其中会引用定义好的时间段），最后激活访问控制列表，使其生效。

1.2.1 时间段配置

对时间段的配置有如下内容：配置每天的时分范围、周期范围和日期范围。配置日期范围采用的是年、月、日、时、分的形式，配置周期范围采用的是每周的周几的形式，配置每天的时分范围采用的是每天的几点、几分的形式。

可以使用下面的命令来配置时间段。

请在系统视图下进行下列配置。

表1-2 创建时间段

操作	命令
创建时间段	**time-range** *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] }
删除时间段	**undo time-range** *time-name* [*start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*]]

如果不配置起始时分和结束时分，时间段就是一天内所有的时间。

如果不配置结束日期，时间段就是从配置生效之日起到系统可以表示的最大时间为止。

1.2.2 定义访问控制列表

Quidway 系列交换机支持多种访问控制列表，下面分别介绍如何定义这些访问控制列表。

定义访问控制列表的步骤为：

(1) 进入相应的访问控制列表视图

(2) 定义访问控制列表的子规则

📖 说明

(1) 如果定义 ACL 时不使用参数 **time-range**，则此访问控制列表激活后将在任何时刻都生效。

(2) 在定义 ACL 的子规则时，用户可以多次使用 **rule** 命令给同一个访问控制列表定义多条规则。

(3) 如果 ACL 用于直接下发到硬件中对转发数据进行过滤和流分类，则用户定义的子规则匹配顺序将不起作用。如果 ACL 用于对由软件处理的报文进行过滤和流分类，用户指定的匹配顺序将会有效，并且用户一旦指定某一条访问控制列表子规则的匹配顺序，就不能再更改该顺序。

(4) 缺省情况下，访问控制列表中子规则的匹配顺序为按用户配置顺序进行匹配。

---

1. 定义基本访问控制列表

基本访问控制列表只根据三层源 IP 制定规则，对数据包进行相应的分析处理。

可以使用下面的命令来定义基本访问控制列表。

请在相应视图下进行下列配置。

表1-3 定义基本访问控制列表

操作	命令
进入基本访问控制列表视图（系统视图）	**acl** { **number** *acl-number* | **name** *acl-name* **basic** } [**match-order** { **config** | **auto** }]
定义子规则（基本访问控制列表视图）	**rule** [*rule-id*] { **permit** | **deny** } [**source** *source-addr wildcard* | **any**] [**fragment**] [**time-range** *name*]

操作	命令
删除访问控制列表的一个子规则（基本访问控制列表视图）	**undo rule** *rule-id* [**source**] [**fragment**] [**time-range**]
删除访问控制列表，或者删除全部访问控制列表（系统视图）	**undo acl** { **number** *acl-number* **| name** *acl-name* | **all** }

2. 定义高级访问控制列表

高级访问控制列表根据源 IP、目的 IP、使用的 TCP 或 UDP 端口号、报文优先级等数据包的属性信息制定分类规则，对数据包进行相应的处理。高级访问控制列表支持对三种报文优先级的分析处理：TOS(Type Of Service)优先级、IP 优先级和 DSCP 优先级。

可以使用下面的命令来定义高级访问控制列表。

请在相应视图下进行下列配置。

表1-4 定义高级访问控制列表

操作	命令
进入高级访问控制列表视图（系统视图）	**acl** { **number** *acl-number* | **name** *acl-name* **advanced** } [**match-order** { **config** | **auto** }]
定义子规则（高级访问控制列表视图）	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [**source** *source-addr wildcard* | **any**] [**destination** *dest-addr wildcard* | **any**] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** *type code*] [**established**] [[**precedence** *precedence* | **tos** *tos*]* | **dscp** *dscp*] [**fragment**] [**time-range** *name*]
删除访问控制列表的一个子规则（高级访问控制列表视图）	**undo rule** *rule-id* [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**precedence**] [**tos**] [**dscp**] [**fragment**] [**time-range**]
删除访问控制列表，或者删除全部访问控制列表（系统视图）	**undo acl** { **number** *acl-number* **| name** *acl-name* | **all** }

高级访问控制列表的数字标识取值范围为 3000～3999。

需要注意的是，上面命令中的 *port1*、*port2* 参数指的是各种高层应用使用的 TCP 或者 UDP 的端口号，对于部分常见的端口号，可以用相应的助记符来代替其实际数字，如使用“bgp”来代替 BGP 协议使用的 TCP 端口号 179。

3. 定义二层访问控制列表

二层访问控制列表根据源 MAC 地址、源 VLAN ID、二层协议类型、报文二层接收端口、报文二层转发端口、目的 MAC 地址等二层信息制定规则，对数据进行相应处理。

可以使用下面的命令来定义二层访问控制列表。

请在相应视图下进行下列配置。

表1-5 定义二层访问控制列表

操作	命令
进入二层访问控制列表视图（系统视图）	**acl** { **number** *acl-number* | **name** *acl-name* **link** } [**match-order** { **config** | **auto** }]
定义子规则（二层访问控制列表视图）	**rule** [*rule-id*] { **permit** | **deny** } [*protocol*] [**cos** *vlan-pri*] [**ingress** { { *source-vlan-id* | *source-mac-addr source-mac-wildcard* }* | **any** }] [**egress** { *dest-mac-addr dest-mac-wildcard* | **any** }] [**time-range** *name*]
删除访问控制列表的一个子规则（二层访问控制列表视图）	**undo rule** *rule-id*
删除访问控制列表，或者删除全部访问控制列表（系统视图）	**undo acl** { **number** *acl-number* **| name** *acl-name* **| all** }

二层访问控制列表的数字标识取值范围为 4000～4999。

1.2.3 激活访问控制列表

将访问控制列表定义好后，必须激活之后才能使之生效。本配置用来激活那些对交换机硬件转发的数据进行过滤或分类的访问控制列表。

可以使用下面的命令来激活定义好的访问控制列表。

请在以太网端口视图下进行下列配置。

表1-6 激活 ACL

操作	命令
激活访问控制列表	**packet-filter inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*
取消激活访问控制列表	**undo packet-filter inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*

📖 说明：

本命令支持同时激活二层访问控制列表和 IP 访问控制列表（IP 访问控制列表包括基本访问控制列表、高级访问控制列表），但是要求组合项的动作一致，如果动作冲突（一个是 permit，而另一个是 deny）则不能激活。

1.2.4 访问控制列表显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后访问控制列表的运行情况。用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **reset** 命令可以将有关访问控制列表的统计信息清除。

表1-7 访问控制列表的显示和调试

操作	命令
显示时间段状况。	**display time-range** [**all** | *name*]
显示访问控制列表的详细配置信息。	**display acl config** { **all** | *acl-number* | *acl-name* }
显示访问控制列表的下发应用信息。	**display acl running-packet-filter** { **all | interface** { *interface-name* | *interface-type interface-num* } }
清除访问控制列表的统计信息。	**reset acl counter** { **all** | *acl-number* | *acl-name* }

display acl config 命令显示的匹配信息是由交换机 CPU 处理的匹配信息。用户可以使用命令 **display qos-interface traffic-statistic** 显示交换机转发数据的匹配信息。

具体的参数说明请参见命令手册。

1.3 访问控制列表典型配置案例

1.3.1 高级访问控制列表配置案例

1. 组网需求

公司企业网通过 Switch 的端口实现各部门之间的互连。研发部门的由 GigabitEthernet0/1 端口接入，工资查询服务器的地址为 129.110.1.2。要求正确配置 ACL，限制研发部门在上班时间 8:00 至 18:00 访问工资服务器。

2. 组网图

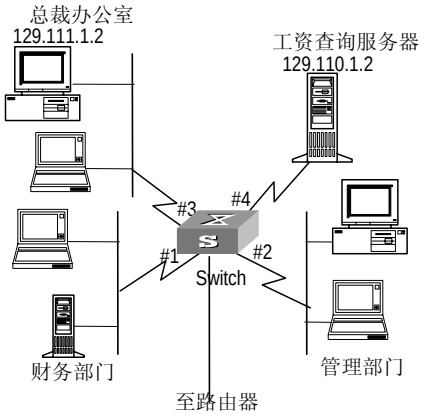


图1-1 访问控制典型配置举例

3. 配置步骤

📖 说明：

以下的配置，只列出了与 ACL 配置相关的命令。

---

(1) 定义时间段

定义 8:00 至 18:00 的周期时间段。

[Quidway] time-range huawei 8:00 to 18:00 working-day

(2) 定义到工资服务器的 ACL

进入基于名字的高级访问控制列表视图，命名为 traffic-of-payserver。

[Quidway] acl name traffic-of-payserver advanced

定义研发部门到工资服务器的访问规则。

[Quidway-acl-adv-traffic-of-payserver] rule 1 deny ip source any destination 129.110.1.2 0.0.0.0 time-range huawei

(3) 激活 ACL。

将 traffic-of-payserver 的 ACL 激活。

[Quidway-GigabitEthernet0/1] packet-filter inbound ip-group traffic-of-payserver

1.3.2 基本访问控制列表配置案例

1. 组网需求

通过基本访问控制列表，实现在每天 8:00～18:00 时间段内对源 IP 为 10.1.1.1 主机发出报文的过滤。该主机从 GigabitEthernet0/1 接入。

2. 组网图

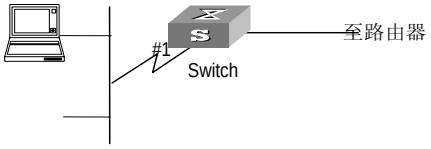


图1-2 访问控制典型配置举例

3. 配置步骤

说明：

以下的配置，只列出了与 ACL 配置相关的命令。

(1) 定义时间段

定义 8:00 至 18:00 的周期时间段。

[Quidway] time-range huawei 8:00 to 18:00 daily

(2) 定义源 IP 为 10.1.1.1 的 ACL

进入基于名字的基本访问控制列表视图，命名为 traffic-of-host。

[Quidway] acl name traffic-of-host basic

定义源 IP 为 10.1.1.1 的访问规则。

[Quidway-acl-basic-traffic-of-host] rule 1 deny ip source 10.1.1.1 0 time-range huawei

(3) 激活 ACL。

将 traffic-of-host 的 ACL 激活。

[Quidway-GigabitEthernet0/1] packet-filter inbound ip-group traffic-of-host

1.3.3 二层访问控制列表配置案例

1. 组网需求

通过二层访问控制列表，实现在每天 8:00～18:00 时间段内对源 MAC 为 00e0-fc01-0101 目的 MAC 为 00e0-fc01-0303 报文的过滤。该主机从 GigabitEthernet0/1 接入。

2. 组网图

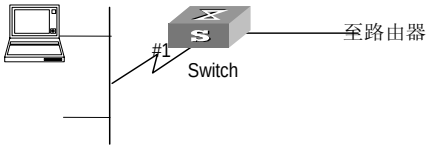


图1-3 访问控制典型配置举例

3. 配置步骤

说明：

以下的配置，只列出了与 ACL 配置相关的命令。

---

(1) 定义时间段

定义 8:00 至 18:00 的周期时间段。

[Quidway] time-range huawei 8:00 to 18:00 daily

(2) 定义源 MAC 为 00e0-fc01-0101 目的 MAC 为 00e0-fc01-0303 的 ACL

进入基于名字的二层访问控制列表视图，命名为 traffic-of-link。

[Quidway] acl name traffic-of-link link

定义源 MAC 为 00e0-fc01-0101 目的 MAC 为 00e0-fc01-0303 的流分类规则。

[Quidway-acl-link-traffic-of-link] rule 1 deny ingress 00e0-fc01-0101 0-0-0 egress 00e0-fc01-0303 0-0-0 time-range huawei

(3) 激活 ACL。

将 traffic-of-link 的 ACL 激活。

[Quidway-GigabitEthernet0/1] packet-filter link-group traffic-of-link

第2章 QoS 配置

2.1 QoS 简介

传统的分组网络对所有报文都无区别的等同对待。每个交换机/路由器对所有的报文采用先入先出的策略（FIFO）处理，尽最大的努力（Best-Effort）将报文送到目的地，但对报文传送的延时、延时抖动等传输性能不提供任何承诺和保证。

随着计算机网络的高速发展，对带宽、延迟、抖动敏感的语音、图像、重要数据越来越多地在网上传输。这样一方面使得网上的业务资源极大地丰富，另一方面则由于经常遭遇网络拥塞，人们对网络传输的服务质量 QoS（Quality of Service）提出了更高的要求。

以太网技术是当今被广泛使用的网络技术。目前，以太网不仅成为各种独立的局域网中的主导技术，许多以太网形式的局域网也成为了 Internet 的组成部分。而且随着以太网技术的不断发展，以太网接入方式也将成为广大普通 Internet 用户的主要接入方式之一。因此要实现端到端的全网 QoS 解决方案，不可避免地要考虑以太网上的 QoS 业务保证的问题。这就需要以太网交换设备应用以太网 QoS 技术，对不同类型的业务流提供不同等级的 QoS 保证，尤其是能够支持那些对延时和抖动要求较高的业务流。

下面介绍 QoS 的一些术语和概念。

1. 流

流即业务流（traffic），指所有通过交换机的报文。

2. 流分类

流分类（traffic classification）是指采用一定的规则识别出符合某类特征的报文。分类规则（classification rule）指配置管理员根据管理需求配置的过滤规则。分类规则可以很简单，比如可根据 IP 报文头的 ToS 字段，识别出有不同优先级特征的流量；也可以很复杂，如综合链路层（Layer 2）、网络层（layer 3）、传输层（layer 4）信息诸如 MAC 地址、IP 协议、源地址、目的地址、或应用程序的端口号等相关信息来对报文进行分类。一般的分类依据都局限在封装报文的头部信息，使用报文的内容作为分类的标准比较少见。

3. 包过滤

包过滤就是将业务流进行过滤操作。例如丢弃操作（deny），该操作将匹配流分类规则的业务流丢弃，而允许其他所有流量通过。以太网交换机采用了复杂的流分类规则，这样可以针对业务流的各种信息进行过滤，丢弃那些无用的、不可靠、值得怀疑的业务流，从而增强了网络的安全性。

实现包过滤，有两个关键的环节：

第一步：是对进入端口的流量按即定的规则进行流分类；

第二步：对区分出来的流进行过滤——丢弃操作（deny）。deny 为缺省的访问控制操作。

4. 流量监管

为了使有限的网络资源可以更好地为用户服务，QoS 在输入端口上可以对特定用户的业务流进行监管，使之适应分配给它的那部分网络资源。

5. 端口限速

端口限速就是基于端口的速率限制，它对端口输出报文的总速率进行限制。

6. 重定向

用户可以基于自身 QoS 策略的需要，重新指定报文的转发端口。

7. 优先级标记

以太网交换机可为特定报文提供优先级标记的服务，标记内容包括 TOS、DSCP、802.1p 等，这些优先级标记分别适用于不同的 QoS 模型，在不同的模型中被定义。

下面介绍一下 IP 优先级、TOS 优先级、DSCP 优先级和 802.1p 优先级。

(1) IP 优先级、TOS 优先级和 DSCP 优先级

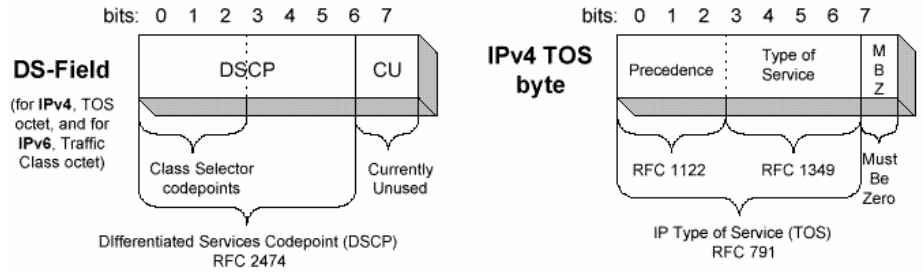


图2-1 DS 域和 ToS 字节

如图 2-1 所示，IP header 的 TOS 字段有 8 个 bit，其中前 3 个 bit 表示的就是 IP 优先级，取值范围为 0～7；第 3～6 这 4 个 bit 表示的是 TOS 优先级，取值范围为 0～15；在 RFC2474 中，重新定义了 IP 报文头部的 TOS 域，称之为 DS 域，其中 DSCP 优先级用该域的前 6 位（0-5 位）表示，取值范围为 0～63，后 2 位（6、7 位）是保留位。

(2) 802.1p 优先级

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。

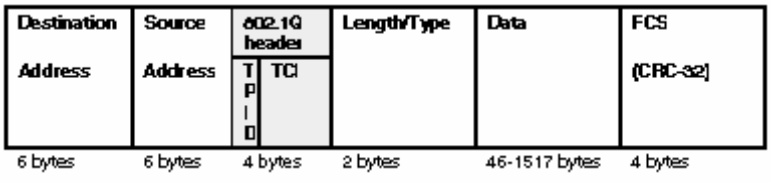


图2-2 带有 802.1Q 标签头的以太网帧

如上图所示，每一个支持 802.1Q 协议的主机，在发送数据包时，都在原来的以太网帧头中的源地址后增加了一个 4 字节的 802.1Q 标签头。

这 4 个字节的 802.1Q 标签头包含了 2 个字节的标签协议标识（TPID--Tag Protocol Identifier，它的值是 8100），和 2 个字节的标签控制信息（TCI--Tag Control Information），TPID 是 IEEE 定义的新的类型，表明这是一个加了 802.1Q 标签的报文，下图显示了 802.1Q 标签头的详细内容。

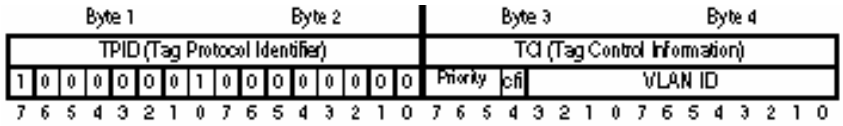


图2-3 802.1Q 标签头

在上图中，TCI 字节中 Priority 字段就是 802.1p 优先级，它由 3 个 bit 组成，取值范围为 0～7。这 3 位指明帧的优先级。一共有 8 种优先级，主要用于当交换机阻塞时，优先发送哪个数据包。

之所以称此优先级为 802.1p 优先级，是因为有关这些优先级的应用是在 802.1p 规范中被详细定义。

8. 队列调度

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。这里介绍 3 种各具特色的队列调度算法：严格优先级 SP

（Strict-Priority）队列调度算法、加权轮循 WRR（Weighted Round Robin）调度算法和带最大时延的 WRR 调度算法。

(1) SP 调度算法

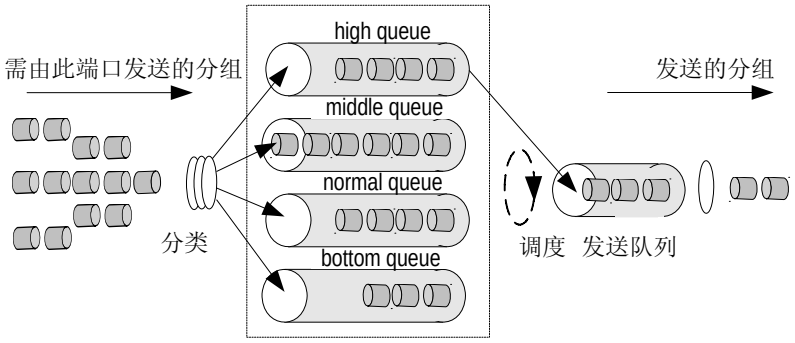


图2-4 优先队列示意图

SP 队列调度算法，是针对关键业务型应用设计的。关键业务有一重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以端口有 4 个输出队列为例，优先队列将端口的 4 个输出队列分成 4 类，分别为高优先队列、中优先队列、正常优先队列和低优先队列（依次为 3、2、1、0 队列），它们的优先级依次降低。

在队列调度时，SP 严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如 E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

(2) WRR 调度算法

交换机的端口支持 4 个或 8 个输出队列，WRR 队列调度算法在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 4 个优先级队列为例，WRR 可为每个队列配置一个加权值（依次为 w3、w2、w1、w0），加权值表示获取资源的比重。如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 50、30、10、10（依次对应 w3、w2、w1、w0），这样可以保证最低优先级队列至少获得 10Mbit/s 带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。WRR 队列还有一个优点是，虽然多个队列的调度是轮循进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

9. 流镜像

流镜像，即能将指定的数据包复制到监控端口，以进行网络检测和故障排除。

10. 端口镜像

端口镜像，即能将指定端口的数据包复制到监控端口，以进行网络检测和故障排除。

11. 基于流的流量统计

基于流的流量统计，针对用户感兴趣的报文作统计分析。

2.2 QoS 配置

QoS 配置包括：

- 设置端口的优先级
- 包过滤
- 流量监管
- 速率限制
- 重定向配置
- 优先级标记
- 队列调度
- 流镜像
- 流量统计

最好首先定义相应的访问控制列表，才能进行以上的 QoS 配置。包过滤配置通过激活相应的访问控制列表就可以实现，本章就不再说明。

2.2.1 设置端口的优先级

可以使用下面的命令设置端口优先级。默认情况下，交换机将使用端口优先级代替该端口接收报文本身带有的 802.1p 优先级，从而控制报文可以享有的服务质量。

请在以太网端口视图下进行下列配置。

表2-1 设置端口的优先级

操作	命令
设置端口的优先级	**priority** *priority-level*
恢复端口的优先级为缺省值	**undo priority**

以太网交换机的端口支持 8 个优先级。用户可以根据需要设置端口的优先级。

priority-level 的取值范围为 0～7。

缺省情况下，端口优先级为 0；对于接收的报文，交换机将使用报文接收端口的优先级替换报文的 802.1p 优先级。

2.2.2 流量监管

流量监管是基于流的速率限制，它可以监督某一流量的速率，如果流量超出指定的规格，就采用相应的措施，如丢弃那些超出规格的报文或重新设置它们的优先级。

可以使用下面的命令来配置流量监管。

请在以太网端口视图下进行下列配置。

表2-2 速率限制配置

操作	命令
基于流的速率限制配置	**traffic-limit inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }* *target-rate* [**exceed** *action*]
取消基于流的速率限制配置	**undo traffic-limit inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*

在进行此项配置之前一定要先定义相应的访问控制列表。

本配置任务的目的是对匹配访问控制列表的数据流实现流量监管：数据的流量超过设定流量采取另外的动作，如丢弃报文。

关于命令的详细描述请参见本章相应的命令手册。

2.2.3 端口限速

端口限速就是基于端口的速率限制，它对端口输出报文的总速率进行限制。

可以使用下面的命令进行端口限速配置。

请在以太网端口视图下进行下列配置。

表2-3 端口限速配置

操作	命令
基于端口的速率限制配置	**line-rate** *target-rate*
取消基于端口的速率限制配置	**undo line-rate**

以太网交换机支持对单个端口的端口限速。

关于命令的详细描述请参见本章对应的命令手册。

2.2.4 报文重定向配置

报文重定向就是用户改变转发的报文的输出方向，将其输出到 CPU 或者输出到其他端口。

可以使用下面的命令来进行报文重定向配置。

请在系统视图下进行下列配置。

表2-4 重定向配置

操作	命令
重定向配置	**traffic-redirect inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }* { **cpu** | **interface** { *interface-name* | *interface-type interface-num* } }
取消重定向配置	**undo traffic-redirect inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*

需要注意的是，当报文被重定向到 CPU 后，将不再正常转发。

📖 **说明：**

重定向配置仅对访问列表中动作为 **permit** 的规则有效。

关于命令的详细描述请参见本章对应的命令手册。

2.2.5 优先级标记配置

优先级标记配置就是为匹配访问控制列表的报文重新标记优先级的策略，所标记的优先级可以填入报文头部反映优先级的域中。

可以使用下面的命令来进行优先级标记配置。

请在系统视图下进行下列配置。

表2-5 标记报文优先级

操作	命令
标记报文优先级	**traffic-priority inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }* { { **cos** *pre-value* | { **dscp** *dscp-value* | **ip-precedence** *pre-value* } | **local-precedence** *pre-value* }* | { { **ip-precedence from-cos** | **cos from-ipprec** } | **local-precedence** *pre-value* }* }
取消标记报文优先级的配置	**undo traffic-priority inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*

以太网交换机支持为报文打上 IP 优先级（**traffic-priority** 命令中的 **ip-precedence** 指定的值）、DSCP 优先级（**traffic-priority** 命令中的 **dscp** 指定的值）、802.1p 优先级（即 **traffic-priority** 命令中的 cos 值）。用户可以根据实际的 QoS 的策略要求给报文打上不同的优先级。交换机根据报文的 802.1p 优先级将报文放入对应的端口输出队列。

关于命令的详细描述请参见本章对应的命令手册。

2.2.6 队列调度配置

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。交换机依据报文的 802.1p 优先级进行入队列操作。802.1p 优先级和队列之间的映射关系如下表所示。

表2-6 802.1p 优先级和队列之间的映射关系

802.1p 优先级	队列
0	2
1	0
2	1
3	3
4	4

802.1p 优先级	队列
5	5
6	6
7	7

可以使用下面的命令来进行队列调度配置。

请在系统视图下进行下列配置。

表2-7 设置队列调度算法

操作	命令
设置队列调度算法	**queue-scheduler** { **rr** | **strict-priority** | **wrr** *queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight queue8-weight* }
恢复队列调度算法的缺省值	**undo queue-scheduler**

以太网交换机支持 3 种队列调度模式：严格优先调度、加权轮循调度以及轮循调度。

缺省情况下交换机采用为严格优先调度模式。

关于命令的详细描述请参见本章对应的命令手册。

2.2.7 流镜像配置

流镜像就是将匹配访问控制列表规则的业务流复制到指定的监控端口，用于报文的分析和监视。

可以使用下面的命令进行流镜像配置。

请在以太网端口视图下进行下列配置。

表2-8 流镜像配置

操作	命令
流镜像配置	**mirrored-to inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*
取消流镜像的配置	**undo mirrored-to inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*

关于命令的详细描述请参见本章对应的命令手册。

2.2.8 端口镜像配置

端口镜像就是将被监控端口上的数据复制到指定的监控端口，对数据进行分析和监视。以太网交换机支持多对一的镜像，即将多个端口的报文复制到一个监控端口上。

用户可以指定受监控的报文的方向，如下所示：

- 只监控指定端口接收的报文
- 只监控指定端口发送的报文
- 同时监控指定端口接收和发送的报文

可以使用下面的命令进行端口镜像配置。

请在系统视图下进行下列配置。

表2-9 端口镜像配置

操作	命令
配置监控端口	**monitor-port** { *interface_name* | *interface_type interface_num* }
配置被监控端口	**mirroring-port** *port-list* { **inbound** | **outbound** | **both** }
取消被监控端口的配置	**undo mirroring-port** *port-list* { **inbound** | **outbound** | **both** }
取消监控端口的配置	**undo monitor-port** { *interface-name* | *interface-type interface-num* }

在配置端口镜像的时候，必须首先配置监控端口，然后配置被监控端口；在取消端口镜像配置时，必须在取消了所有被监控端口的配置之后才能取消监控端口的配置。

📖 说明

在取消被监控端口的配置时也可以指定报文的方向:
(1) 只取消对端口接收报文的监控
(2) 只取消对端口发送报文的监控
(3) 同时取消对端口接收和发送报文的监控
需注意，如果配置被监控端口时指定了对端口接收和发送的报文都进行监控，而在取消该被监控端口的配置时只取消对该被监控端口接收报文的监控，则交换机仍然对该被监控端口发送的报文进行监控。此时不能删除监控端口。

关于命令的详细描述请参见本章对应的命令手册。

2.2.9 流量统计配置

流量统计用于统计指定业务流的数据包，它统计的是交换机转发的数据包中匹配已定义的访问控制列表的数据信息。在进行了流量统计配置之后，用户可以使用命令 **display qos-interface traffic-statistic** 显示统计的信息。

可以使用下面的命令来进行流量统计配置。

请在以太网端口视图下进行下列配置。

表2-10 流量统计配置

操作	命令
流量统计配置	**traffic-statistic inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*
取消流量统计配置	**undo traffic-statistic inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }*
显示流量统计信息	**display qos-interface** [*interface-name* | *interface-type interface-num*] **traffic-statistic**

关于命令的详细描述请参见本章对应的命令手册。

2.2.10 QoS 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后 QoS 的运行情况。用户可以通过查看显示信息验证配置的效果。在以太网端口视图下执行 **reset** 命令可以将有关 QoS 的统计信息清除。

表2-11 QoS 的显示和调试

操作	命令
显示所有 QoS 动作的参数设置	**display qos-global all**
显示流镜像的参数设置	**display qos-interface** [*interface-name* | *interface-type interface-num*] **mirrored-to**
显示端口镜像的参数设置	**display mirror**
显示队列调度模式及参数	**display queue-scheduler**
显示所有端口的 QoS 设置信息	**display qos-interface** [*interface-name* | *interface-type interface-num*] **all**
显示流量限制的参数设置	**display qos-interface** [*interface-name* | *interface-type interface-num*] **traffic-limit**
显示端口限速的参数设置	**display qos-interface** [*interface-name* | *interface-type interface-num*] **line-rate**
显示优先级标记的参数设置	**display qos-interface** [*interface-name* | *interface-type interface-num*] **traffic-priority**
显示重定向的参数设置	**display qos-interface** [*interface-name* | *interface-type interface-num*] **traffic-redirect**
显示流量统计信息	**display qos-interface** [*interface-name* | *interface-type interface-num*] **traffic-statistic**
统计信息清零	**reset traffic-statistic inbound** { **all** | { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }* }

相关命令显示信息及说明请参见命令手册。

2.2.11 QoS 配置示例

1. 组网需求

公司企业网通过以太网交换机的端口实现各部门之间的互连。财务部门的工资查询服务器由 GigabitEthernet0/1 端口接入（子网地址 129.110.1.2）。组网需求为要求限制其它部门访问工资服务器的流量为 20M，限制工资服务器向外发送流量的平均速率不能超过 20M，超出规格的报文将报文优先级为 4。

2. 组网图

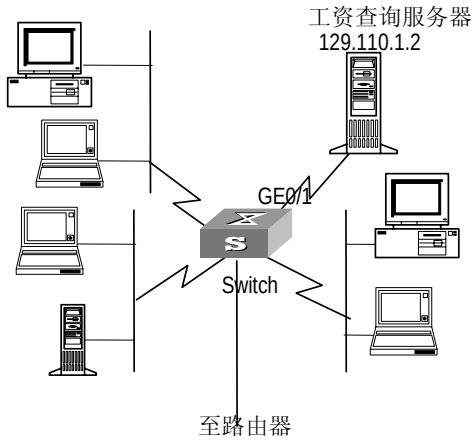


图2-5 QoS 配置举例

3. 配置步骤

说明：

以下的配置，只列出了与 QoS/ACL 配置相关的命令。

(1) 定义工资服务器向外发送的流量

进入基于名字标识的高级访问控制列表视图，用 traffic-of-payserver 标识。

[Quidway] acl name traffic-of-payserver advanced

定义 traffic-of-payserver 这条高级访问控制列表的规则。

[Quidway-acl-adv-traffic-of-payserver] rule 1 permit ip source 129.110.1.2 0.0.0.0 destination any

(2) 对访问工资服务器的流量进行流量限制

限制工资服务器向外发送报文的平均速率为 20M，对超出规格的报文设置优先级为 4。

[Quidway-GigabitEthernet0/1] traffic-limit inbound ip-group traffic-of-payserver 20 exceed remark-dscp 4

限制端口 GigabitEthernet0/1 发往工资服务器的速率为 20M。

[Quidway-GigabitEthernet0/1] line-rate 20

第3章 配置登录用户的 ACL 控制

3.1 简介

随着以太网交换机设备在网上日益广泛应用，安全问题愈显突出。目前，以太网交换机提供了多种用户登录、访问设备的方式，主要有通过 SNMP（Simple Network Management Protocol）访问、通过 TELNET 访问和通过 HTTP（Hypertext Transfer Protocol）访问三种方式。以太网交换机提供对这三种访问方式进行安全控制的特性，防止非法用户登录、访问交换机设备。安全控制分为两级，第一级安全通过控制用户的连接实现，通过配置 ACL（Access Control List）对登录用户进行过滤，只有合法用户才能和交换机设备建立连接；第二级安全主要通过用户口令认证实现，连接到设备的用户必须通过口令认证才能真正登录到设备。

本节将介绍如何配置这些主要访问方式的第一级安全控制，即怎样配置对登录交换机设备用户进行 ACL 控制。第二级安全的配置请参见手册的入门模块。

3.2 配置对 TELNET 用户的 ACL 控制

通过配置对 TELNET 用户的 ACL 控制，可以在进行口令认证之前将一些恶意或者不合法的连接请求过滤掉，保证设备的安全。

配置对 TELNET 用户的 ACL 控制需要下面两个步骤：

(1) 定义访问控制列表

(2) 引用访问控制列表，对 TELNET 用户进行控制

下面介绍配置过程。

3.2.1 定义访问控制列表

目前，ACL 控制功能能够引用的访问控制列表只能是基于数字标识的基本访问控制列表，数字的取值范围为 2000～2999。

可以使用下面的命令定义基本访问控制列表。

请在系统视图下进行下列配置。

表3-1 定义基本访问控制列表

操作	命令
进入基本访问控制列表视图（系统视图）	**acl** { **number** *acl-number* | **name** *acl-name* **basic** } **match-order** { **config** | **auto** }
定义子规则（基本访问控制列表视图）	**rule** [*rule-id*] { **permit** | **deny** } [**source** *source-addr wildcard* | **any**] [**fragment**] [**time-range** *name*]
删除访问控制列表的一个子规则（基本访问控制列表视图）	**undo rule** *rule-id* [**source**] [**fragment**] [**time-range**]
删除访问控制列表，或者删除全部访问控制列表（系统视图）	**undo acl** { **number** *acl-number* **| name** *acl-name* | **all** }

在定义过程中，可以多次使用 **rule** 命令给同一个访问控制列表定义多条规则。

3.2.2 引用访问控制列表，对 TELNET 用户进行控制

在交换机的用户界面视图下引用定义好的访问控制列表，就可以实现对 TELNET 用户的 ACL 控制。

可以使用下面的命令来引用访问控制列表。

请在相应视图下进行下列配置。

表3-2 引用访问控制列表，对 TELNET 用户进行控制

操作	命令
进入用户界面视图（系统视图）	**user-interface** [*type*] *first-number* [*last-number*]
引用访问控制列表（用户界面视图）	**acl** *acl-number* { **inbound** | **outbound** }

关于命令的详细描述请参见命令手册。

📖 **说明：**

TELNET 用户的 ACL 控制功能只能引用基于数字标识的基本访问控制列表。

3.2.3 配置举例

1. 组网需求

仅允许来自 10.110.100.52 和 10.110.100.46 的 TELNET 用户访问交换机。

2. 组网图

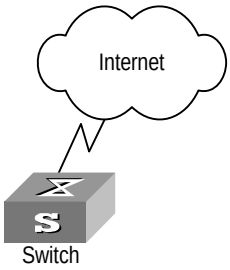


图3-1 对 Switch 的 TELNET 用户进行 ACL 控制

3. 配置步骤

定义基本访问控制列表。

[Quidway] acl number 2000 match-order config

[Quidway-acl-basic-2000] rule 1 permit source 10.110.100.52 0

[Quidway-acl-basic-2000] rule 2 permit source 10.110.100.46 0

[Quidway-acl-basic-2000] quit

引用访问控制列表。

[Quidway] user-interface vty 0 4

[Quidway-user-interface-vty0-4] acl 2000 inbound

3.3 对通过 SNMP 访问交换机的用户的 ACL 控制

华为 Quidway 系列以太网交换机支持通过网管软件进行远程管理。网管用户可以通过 SNMP 访问交换机，对这些用户的 ACL 控制功能可以过滤掉不合法的网管用户，使其不能登录本交换机。

配置对通过 SNMP 访问交换机的用户的 ACL 控制需要下面两个步骤：

(1) 定义访问控制列表

(2) 引用访问控制列表，对通过 SNMP 访问交换机的用户进行控制

下面介绍配置过程。

3.3.1 定义访问控制列表

目前，ACL 控制功能能够引用的访问控制列表只能是基于数字标识的基本访问控制列表，数字的取值范围为 2000～2999。具体配置命令和上一节完全一样。

3.3.2 引用访问控制列表，对通过 SNMP 访问交换机的用户进行控制

在配置 SNMP 的团体名、用户名、组名的命令中引用定义好的访问控制列表，就可以实现对网管用户的 ACL 控制。

可以使用下面的命令来引用访问控制列表。

请在系统视图下进行下列配置。

表3-3 对通过 SNMP 访问交换机的用户进行控制

操作	命令
在配置 SNMP 团体名的命令中引用访问控制列表	**snmp-agent community** { **read** | **write** } *community-name* [[**mib-view** *view-name*] | [**acl** *acl-number*]]*
在配置 SNMP 组名的命令中引用访问控制列表	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]
在配置 SNMP 用户名的命令中引用访问控制列表	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password*] [**privacy-mode des56** *priv-password*] [**acl** *acl-number*]

SNMP 团体名属性是 SNMP V1、SNMP V2 版本的一个特性，所以在配置 SNMP 团体名的命令中引用访问控制列表对使用 SNMP V1、SNMP V2 的网管系统起到过滤作用。

SNMP 组名、用户名属性是 SNMP V2 及以上版本的一个特性，所以在配置 SNMP 组名、用户名的命令中引用访问控制列表对使用 SNMP V2 及以上版本的网管系统起到过滤作用。如果同时在这两个命令中配置了 ACL 控制功能，则交换机会对网管用户的这两个属性都进行过滤。

📖 说明：

以上三个命令中引用的访问控制列表可以是不同的访问控制列表。

关于命令的详细描述请参见命令手册。

📖 说明：

网管用户的 ACL 控制功能只能引用基于数字标识的基本访问控制列表。

3.3.3 配置举例

1. 组网需求

仅允许来自 10.110.100.52 和 10.110.100.46 的 SNMP 用户访问交换机。

2. 组网图

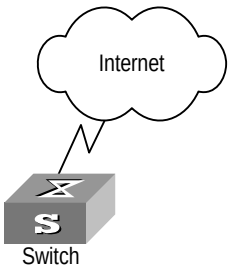


图3-2 对 Switch 的 SNMP 用户进行 ACL 控制

3. 配置步骤

定义基本访问控制列表。

[Quidway] acl number 2000 match-order config

[Quidway-acl-baisc-2000] rule 1 permit source 10.110.100.52 0

[Quidway-acl-baisc-2000] rule 2 permit source 10.110.100.46 0

[Quidway-acl-baisc-2000] quit

引用访问控制列表。

[Quidway] snmp-agent community read huawei acl 2000

[Quidway] snmp-agent group v2c huaweigroup acl 2000

[Quidway] snmp-agent usm-user v2c huaweiuser huaweigroup acl 2000

3.4 对通过 HTTP 访问交换机的用户的 ACL 控制

华为 Quidway 系列以太网交换机支持通过 WEB 进行远程管理。用户可以通过 HTTP 访问交换机。对这些用户的 ACL 控制功能可以过滤掉不合法的用户，使其不能登录本交换机。在配置了对这些用户的 ACL 控制功能以后，交换机同一时刻将只允许一名 WEB 用户访问以太网交换机。

配置对通过 HTTP 访问交换机的用户的 ACL 控制需要下面两个步骤：

(1) 定义访问控制列表

(2) 引用访问控制列表，对通过 HTTP 访问交换机的用户进行控制

下面介绍配置过程。

3.4.1 定义访问控制列表

目前，ACL 控制功能能够引用的访问控制列表只能是基于数字标识的基本访问控制列表，数字的取值范围为 2000～2999。具体配置命令和上一节完全一样。

3.4.2 引用访问控制列表，对通过 HTTP 访问交换机的用户进行控制

通过引用定义好的访问控制列表，就可以实现对 WEB 网管用户的 ACL 控制。

可以使用下面的命令来引用访问控制列表。

请在系统视图下进行下列配置。

表3-4 引用访问控制列表，对通过 HTTP 访问交换机的用户进行控制

操作	命令
引用访问控制列表对 WEB 网管用户进行 ACL 控制	**ip http acl** *acl-number*
取消 ACL 控制功能	**undo ip http acl**

关于命令的详细描述请参见命令手册。

📖 **说明：**

WEB 网管用户的 ACL 控制功能只能引用基于数字标识的基本访问控制列表。

3.4.3 配置举例

1. 组网需求

仅允许来自 10.110.100.46 的 HTTP 用户访问交换机。

2. 组网图

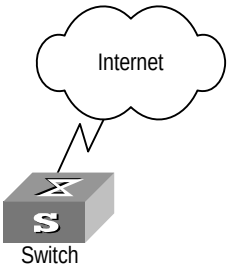


图3-3 对 Switch 的 HTTP 用户进行 ACL 控制

3. 配置步骤

定义基本访问控制列表。

[Quidway] acl number 2030 match-order config

[Quidway-acl-basic-2030] rule 1 permit source 10.110.100.46 0

引用访问控制列表。

[Quidway] ip http acl 2030

目 录

第1章 堆叠功能配置

1.1 堆叠功能简介

堆叠是由一些通过堆叠口相连的以太网交换机组成的一个管理域，其中包括一个主交换机和若干个从交换机。堆叠在一起的以太网交换机可看作为一个设备，用户可通过主交换机实现对堆叠内所有交换机的管理。

当多个以太网交换机通过堆叠口相连时，用户可以在其中一台进行配置，把它们设置成堆叠，并把当前进行配置的以太网交换机设置为堆叠中的主交换机。

堆叠的建立过程如下：主交换机和从交换机之间通过堆叠模块及特殊的堆叠线连接起来（关于堆叠模块及堆叠线的描述请参见安装手册）。用户首先设置堆叠可选的 IP 地址范围，并启用堆叠功能；然后系统会自动将与主交换机堆叠口相连的交换机加入到堆叠中。主交换机在从交换机加入堆叠时，自动给从交换机分配可用的 IP 地址。在建立了堆叠后，如果有新的交换机和主交换机通过堆叠口相连，系统将自动把新的交换机加入到堆叠中。

堆叠是通过主交换机和从交换机之间的连接来维持的。只要发现连接断开，从交换机自动退出堆叠。

1.2 堆叠功能配置

堆叠功能主要配置包括：

- 配置堆叠 IP 地址池
- 建立/删除堆叠
- 切换到从交换机视图进行配置

1.2.1 配置堆叠 IP 地址池

在建立堆叠前，用户需首先设置堆叠可选的 IP 地址范围，主交换机将在从交换机加入堆叠时，自动给从交换机分配已设置的 IP 地址范围内的 IP 地址。

请在系统视图下进行下列配置。

表1-1 配置堆叠 IP 地址池

操作	命令
配置堆叠 IP 地址范围	**stacking ip-pool** *from-ip-address ip-address-number* [*ip-mask*]
恢复堆叠缺省的 IP 地址范围	**undo stacking ip-pool**

在进行堆叠配置前，用户必须首先配置 IP 地址池。同时，用户应该在将成为主交换机的交换机上配置 IP 地址池。

需要注意的是，本配置只能在非堆叠交换机上使用。如果堆叠已经建立，则用户不能修改 IP 地址范围。

缺省情况下，系统没有默认的 IP 地址池。用户必须首先给交换机配置 IP 地址池，然后才能进行堆叠配置。

1.2.2 建立/删除堆叠

当用户使用以下命令建立堆叠时，系统会自动将与主交换机堆叠口相连的交换机加入到堆叠中。堆叠建立后，如果堆叠口连接断开，则从交换机自动退出堆叠。

请在系统视图下进行下列配置。

表1-2 建立/删除堆叠

操作	命令
建立堆叠	**stacking enable**
删除堆叠	**undo stacking enable**

需要注意的是，建立/删除堆叠操作只能在堆叠主交换机上进行。

1.2.3 切换到从交换机视图进行配置

可以使用以下命令从堆叠主交换机视图切换到从交换机视图，从而对从交换机进行配置。

请在用户视图下进行下列配置。

表1-3 切换到从交换机视图进行配置

操作	命令
切换到从交换机视图进行配置	**stacking** *num*

需要注意的是，本命令仅可以从主交换机视图切换到从交换机视图，且切换时用户级别不变。如果从从交换机视图切换回主交换机视图，则只需输入 **quit** 即可。

1.3 堆叠功能显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后堆叠功能的运行情况。用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **reset** 命令可以将有关堆叠的统计信息清除。

表1-4 堆叠功能的显示和调试

操作	命令
在主交换机上显示堆叠状态信息	**display stacking** [**members**]
在从交换机上显示堆叠状态信息	**display stacking**

在主交换机上使用该命令时，如不带 **members**，将显示本交换机是堆叠的主交换机以及堆叠中包含的交换机数目；如带 **members**，将显示堆叠的成员信息，包括主/从交换机的堆叠号、堆叠的设备名称、MAC 地址以及状态等。

在从交换机上使用此命令时，将显示本交换机是堆叠的从交换机、本交换机的堆叠号、堆叠中主交换机的 MAC 地址。

显示命令的显示信息及说明请参见命令手册。

1.4 堆叠功能配置举例

1. 组网需求

Switch A 与 Switch B、Switch C 通过堆叠口相连，组成一个堆叠组。Switch A 作为主交换机，Switch B、Switch C 作为从交换机，网络管理员通过 Switch A 实现对 Switch B、Switch C 的管理。

2. 组网图

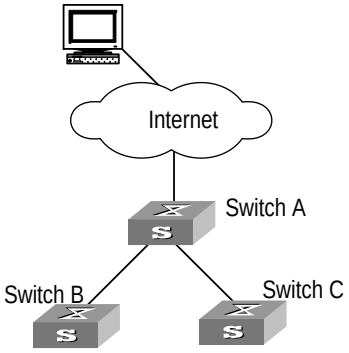


图1-1 配置堆叠功能示例图

3. 配置步骤

在交换机 Switch A 上配置堆叠 IP 地址池。

[Quidway] stacking ip-pool 129.10.1.1 5

在交换机 Switch A 上建立堆叠。

[Quidway] stacking enable

在主交换机 Switch A 上显示堆叠信息。

<stack_0. Quidway> display stacking

```
Main device for stack.
Total members:3
```

在主交换机 Switch A 上显示堆叠成员信息。

<stack_0. Quidway> display stacking members

```
Member number: 0
Name:stack_0.Quidway
Device:Quidway S3526
MAC Address:00e0.fc07.0bc0
Member status:Cmdr

Member number: 1
Name:stack_1.Quidway
Device:Quidway S3026
MAC Address:00e0.fc07.58a0
Member status:Up

Member number: 2
```

```
Name:stack_2.Quidway
Device:Quidway S5024
MAC Address:00e0.fc07.58a1
Member status:Up
```

切换到从交换机 Switch B 上进行配置。

<stack_0. Quidway> stacking 1

<stack_1. Quidway>

在从交换机 Switch B 上显示堆叠信息。

<stack_1. Quidway> display stacking

```
Slave device for stack.
Member number: 1
Main switch mac address:00e0.fc07.0bc0
```

切换回主交换机 Switch A 上进行配置。

<stack_1. Quidway> quit

<stack_0. Quidway>

切换到从交换机 Switch C 上进行配置。

<stack_0. Quidway> stacking 2

<stack_2. Quidway>

切换回主交换机 Switch A 上进行配置。

<stack_2. Quidway> quit

<stack_0. Quidway>

第2章 HGMP V2 配置

2.1 HGMP V2 简介

2.1.1 简介

使用 HGMP V2 功能，网络管理员可以通过一个主交换机的公网 IP 地址，实现对多个交换机的管理。主交换机称为管理设备，其它被管理的交换机称为成员设备。成员设备一般不设置公网 IP 地址，通过管理设备重定向来实现对成员设备的管理和维护。管理设备和成员设备组成了一个“集群”。典型的应用环境如下图所示：

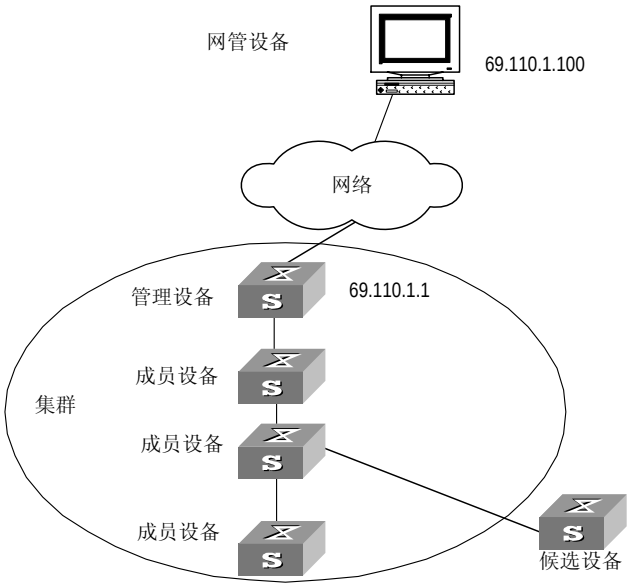


图2-1 集群

2.1.2 交换机的角色

根据集群中各交换机所处的地位和功能的不同，形成了不同的角色，用户可以通过配置来指定交换机的角色，各种角色可以按一定的规则进行切换。

集群中的角色有管理设备、成员设备以及候选设备。

- 管理设备：配置有公网 IP 地址，为集群内所有的交换机提供管理接口的交换机。管理设备通过命令重定向来对成员设备进行管理：用户通过公

网将管理命令发送到管理设备上，由管理设备处理；管理设备如果发现此命令是送往某个成员设备上执行的命令，则将此命令转发到成员设备上处理。管理设备具有发现邻接信息、收集整个网络的拓扑结构、管理集群、维护集群状态、支持各种代理等功能。

- 成员设备：集群中的成员，一般不配置公网 IP 地址。用户通过管理设备的命令重定向功能对成员设备进行管理。成员设备具有发现邻接信息、接受管理设备的管理、执行代理发过来的命令、故障/日志上报等功能。
- 候选设备：没有加入任何集群中但具有集群能力、能够成为集群成员的交换机。

角色转换规则如下：

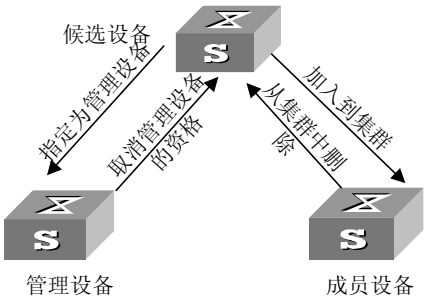


图2-2 角色切换规则

- 每个集群必须指定一个（而且只能指定一个）管理设备。在管理设备被指定后，管理设备通过收集 NDP/NTDP 信息，确定和发现候选设备。用户可以通过相应的配置把候选设备加入到集群中。
- 候选设备加入集群后，成为成员设备；成员设备被删除后将恢复为候选设备。

📖 **说明：**

在集群功能的配置中，管理设备上需要作如下配置：

（1）启动系统和端口上的 NDP

（2）配置 NDP 的参数

（3）启动系统和端口上的 NTDP

（4）配置 NTDP 参数

（5）启动集群功能

（6）配置集群的参数

成员设备和候选设备上需要作如下配置：

（1）启动系统和端口上的 NDP

（2）启动系统和端口上的 NTDP

（3）启动集群功能

2.1.3 功能组成

HGMP V2 的优点如下：

- 简化配置管理任务：只需要在管理设备上配置一个公网 IP 地址，就可实现对多个交换机的配置和管理，不需要登录到每个成员设备的配置口上进行配置；
- 提供拓扑发现和显示功能，有助于监视和调试网络；
- 节省 IP 地址；
- 可以同时对多个交换机进行软件升级和参数配置；
- 不受网络拓扑结构和距离的限制。

HGMP V2 包含以下功能：

- 网络拓扑发现
- 网络拓扑收集
- 成员识别
- 成员管理

其中：

- 网络拓扑发现功能是利用 NDP 来实现的，用来发现直接相连的邻居信息，包括邻接设备的设备类型、软/硬件版本、连接端口等，另外还可提供设备的 ID、端口单双工、产品版本、Bootrom 版本等信息。
- 网络拓扑收集功能是利用 NTDP 来实现的，收集网络中各个设备的连接关系和候选设备信息，并可以设置拓扑发现的跳数。
- 成员识别功能是通过对集群中的各个成员的定位，使管理设备可以识别各个成员并向成员分发配置和管理命令。
- 成员管理功能，包括成员的加入、删除、成员设备对管理设备的验证和握手间隔等。

集群管理涉及的各项功能的具体配置，下面将分别介绍。

2.2 NDP 配置

2.2.1 NDP 简介

NDP（Neighbor Discovery Protocol）是用来发现邻接点相关信息的协议。NDP 运行在数据链路层，因此可以支持不同的网络层协议。

NDP 用来发现直接相连的邻居信息，包括邻接设备的设备类型、软/硬件版本、连接端口等，另外还可提供设备的 ID、端口地址、硬件平台等信息。

支持 NDP 的设备都维护 NDP 邻居信息表，邻居信息表中的每一表项都是可以老化的，一旦老化时间到，NDP 自动删除相应的邻居表项。同时，用户可以清除当前的 NDP 信息以重新收集邻接信息。

运行 NDP 的设备定时向所有激活的端口广播带有 NDP 数据的报文，报文中携带有效保留时间，该时间指示接收设备必须保存该更新数据的时间。接收 NDP 报文的设备保存报文中的信息，但不转发 NDP 报文。收到的信息如果与旧的信息不同，则更新 NDP 表中的相应数据项；如果相同，则只更新有效保留时间。

NDP 主要配置包括：

- 使能/禁止系统 NDP
- 使能/禁止端口 NDP
- 配置 NDP 信息的有效保留时间
- 配置 NDP 报文发送的时间间隔

📖 **说明：**

管理设备上需要启动系统和端口上的 NDP，并且配置 NDP 的参数。而成员设备和候选设备上只需要启动系统和相应端口上的 NDP，在协议运行过程中，它们采用管理设备发送过来的 NDP 参数值。

2.2.2 使能/禁止系统 NDP

要收集任何端口邻接设备的 NDP 信息，用户都需要在交换机上使能系统 NDP。当系统 NDP 使能后，交换机将进行 NDP 信息的定时收集，用户可以查询这些信息；当系统 NDP 禁止后，交换机将清除交换机保存的所有 NDP 邻居信息，同时不再处理任何 NDP 报文。

请在系统视图下进行下列配置。

表2-1 使能/禁止系统 NDP

操作	命令
使能系统 NDP	**ndp enable**
禁止系统 NDP	**undo ndp enable**

缺省情况下，系统 NDP 处于使能状态。

2.2.3 使能/禁止端口 NDP

用户可以控制端口 NDP 使能/禁止状态，从而控制对哪些端口进行邻接节点的信息收集，哪些不收集。如果使能端口 NDP，并且启动了系统 NDP，则系统将定时收集该端口邻接节点的 NDP 邻居信息；如果禁止端口 NDP，则系统不能通过该端口收集和发送 NDP 信息。

请在以太网端口视图下进行下列配置。

表2-2 使能/禁止端口 NDP

操作	命令
使能端口 NDP	**ndp enable** [**interface** *port-list*]
禁止端口 NDP	**undo ndp enable** [**interface** *port-list*]

缺省情况下，端口 NDP 处于使能状态。

2.2.4 配置 NDP 信息的有效保留时间

通过本配置，用户可以控制保留在邻接节点中本节点信息的有效保留时间。交换机在接收到 NDP 报文时，可以从报文中携带的有效保留时间知道发送报文的邻接设备的 NDP 信息的有效时间，并在超出有效时间后丢弃该邻接设备的 NDP 邻居信息。

请在系统视图下进行下列配置。

表2-3 配置 NDP 信息的有效保留时间

操作	命令
配置 NDP 信息的有效保留时间	**ndp timer aging** *aging-in-secs*
恢复 NDP 信息的有效保留时间为缺省值	**undo ndp timer aging**

需要注意的是，NDP 信息的有效保留时间一般大于 NDP 发送时间间隔，否则将引起 NDP 信息表的不稳定。

缺省情况下，NDP 信息的有效保留时间为 180 秒。

2.2.5 配置 NDP 报文发送的时间间隔

对邻接节点的 NDP 信息必须实时更新，以保证邻接节点改变后，交换机能够及时更新本地保留的信息。用户可以通过配置 NDP 报文的发送间隔修改 NDP 信息的更新频率，从而使邻接设备及时更新保留的本交换机的信息。

请在系统视图下进行下列配置。

表2-4 配置 NDP 报文发送的时间间隔

操作	命令
配置 NDP 报文发送的时间间隔	**ndp timer hello** *seconds*
恢复 NDP 报文发送的时间间隔为缺省值	**undo ndp timer hello**

需要注意的是，NDP 报文发送时间间隔一般小于 NDP 信息的有效保留时间，否则将引起 NDP 邻居信息表的不稳定。

缺省情况下，NDP 报文发送时间间隔为 60 秒。

2.2.6 NDP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后 NDP 的运行情况。用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **reset** 命令可以将有关 NDP 的统计信息清除。在用户视图下执行 **debugging** 命令可以对 NDP 模块进行调试。

表2-5 NDP 显示和调试

操作	命令
显示系统 NDP 配置信息（包括报文发送时间间隔和信息有效保留时间）	**display ndp**
显示指定端口 NDP 发现的邻居信息	**display ndp interface** *port-list*
清除 NDP 端口的统计信息	**reset ndp statistics** [**interface** *port-list*]
打开/关闭 NDP 调试开关	[**undo**] **debugging ndp packet** [**interface** *port-list*]

显示维护命令的显示信息及说明请参见命令手册。

2.3 NTDP 配置

2.3.1 NTDP 简介

NTDP（Neighbor Topology Discovery Protocol）是用来收集网络拓扑信息的协议。NTDP 为集群管理提供可加入集群的设备信息，收集指定跳数内的交换机的拓扑信息。

NDP 为 NTDP 提供邻接表信息，NTDP 根据邻接信息发送和转发 NTDP 拓扑收集请求，收集一定网络范围内每个设备的 NDP 信息和它与所有邻居的连接信息。收集完这些信息后，管理设备或者网管可以根据需要使用这些信息，完成所需的功能。

当成员设备上的 NDP 发现邻居有变化时，通过握手报文将邻居改变的消息通知管理设备，管理设备可以启动 NTDP 进行指定拓扑收集，从而使 NTDP 能够及时反映网络拓扑的变化。

NTDP 主要配置包括：

- 使能/禁止系统 NTDP
- 使能/禁止端口 NTDP
- 配置拓扑收集范围
- 配置当前设备转发拓扑收集请求的跳数延迟时间和端口延迟时间
- 配置定时拓扑收集的时间间隔
- 启动拓扑信息的手动收集过程

📖 **说明：**

管理设备上需要启动系统和端口上的 NTDP，并且配置 NTDP 的参数。而成员设备和候选设备上只需要启动系统和相应端口上的 NTDP，在协议运行过程中，它们采用管理设备发送过来的 NTDP 参数值。

2.3.2 使能/禁止系统 NTDP

要使设备能够处理 NTDP 报文，必须使能系统 NTDP。当系统 NTDP 禁止后，交换机将清除交换机保存的所有 NTDP 信息，丢弃所有的 NTDP 报文，禁止发送 NTDP 请求。

请在系统视图下进行下列配置。

表2-6 使能/禁止系统 NTDP

操作	命令
使能系统 NTDP	**ntdp enable**
禁止系统 NTDP	**undo ntdp enable**

缺省情况下，系统 NTDP 处于使能状态。

2.3.3 使能/禁止端口 NTDP

用户可以控制 NTDP 端口使能/禁止状态，来控制对哪些端口进行发送、接收和转发 NTDP 报文，哪些端口不处理。如果使能端口 NTDP，且系统 NTDP 也已使能，则交换机可以从该端口发送、接收和转发 NTDP 报文；如果禁止端口 NTDP，交换机不能通过该端口处理 NTDP 报文。

请在以太网端口视图下进行下列配置。

表2-7 使能/禁止端口 NTDP

操作	命令
使能端口 NTDP	**ntdp enable**
禁止端口 NTDP	**undo ntdp enable**

需要注意的是，在某些情况下，收集网络拓扑时，只收集设备下行端口连接的网络拓扑，不关心上行端口连接的网络的拓扑结构，此时需要禁止上行端口的 NTDP。

缺省情况下，支持 NDP 的端口使能 NTDP。如果某端口禁止 NDP，即使使能端口 NTDP，NTDP 仍然不能运行。

2.3.4 配置拓扑收集范围

用户可以在交换机上配置拓扑收集范围，以收集确定范围内设备的拓扑信息，从而避免无限的扩展收集过程。控制收集范围采用从收集发起开始控制允许发现的跳数的方法。例如，如果设置收集范围为 2，意味着当前交换机将收集从本交换机开始两跳内的设备的拓扑信息。

请在系统视图下进行下列配置。

表2-8 配置拓扑收集范围

操作	命令
配置拓扑收集范围	**ntdp hop** *hop-value*
恢复拓扑收集范围为缺省值	**undo ntdp hop**

需要注意的是，只有在发起拓扑收集请求的交换机上进行收集范围的设置才有效。拓扑收集范围越大，占用拓扑收集设备的内存越多。

缺省情况下，拓扑收集范围为 3。

2.3.5 配置当前设备转发拓扑收集请求的跳数延迟时间和端口延迟时间

当拓扑请求报文在网络内扩散时，大量网络设备会同时收到拓扑收集请求，同时发送响应报文，可能会引起网络拥塞和拓扑收集设备繁忙。为了减少这种情况的出现，每个设备在接收到拓扑请求后，延迟等待一定时间后（这个时间为跳数延迟时间），第一个端口再开始转发拓扑请求报文，再延迟等待一定时间（这个时间为端口延迟时间），下一个端口才开始转发拓扑请求报文，依次类推。

可以使用下面的命令来配置当前设备转发拓扑收集请求的跳数延迟时间和端口延迟时间。

请在系统视图下进行下列配置。

表2-9 配置被收集设备及端口转发拓扑收集请求延迟时间

操作	命令
配置当前设备转发拓扑收集请求的跳数延迟时间	**ntdp timer hop-delay** *time*
恢复当前设备转发拓扑收集请求的跳数延迟时间为缺省值	**undo ntdp timer hop-delay**
配置当前设备转发拓扑收集请求的端口延迟时间	**ntdp timer port-delay** *time*
恢复当前设备转发拓扑收集请求的端口延迟时间为缺省值	**undo ntdp timer port-delay**

缺省情况下，当前设备转发拓扑收集请求的跳数延迟时间为 200ms，转发拓扑收集请求的端口延迟时间为 20ms。

2.3.6 配置定时拓扑收集的时间间隔

启动了集群功能后，如果管理设备发现成员设备有变化，会通知 NTDP 进行局部拓扑收集。这种局部收集不能反映出拓扑的全局变化。为了及时发现网络拓扑结构的变化，NTDP 会周期性的进行全局范围内全部设备的拓扑收集，以防止局部收集不能反映出来的拓扑的全部变化。

可以使用下面的命令来配置定时拓扑收集的周期。

请在系统视图下进行下列配置。

表2-10 配置定时拓扑收集的时间间隔

操作	命令
配置定时拓扑收集的时间间隔	**ntdp timer** *interval-in-mins*
恢复定时拓扑收集的时间间隔为缺省值	**undo ntdp timer**

缺省情况下，定时拓扑收集的时间间隔为 0 分钟，即不进行定时拓扑收集。

2.3.7 启动拓扑信息的手动收集过程

当配置了拓扑收集的时间间隔后，NTDP 会自动以此时间间隔为周期，定时进行全部范围内拓扑信息的收集过程。另外 NTDP 还提供给用户手动收集网络拓扑信息的命令，以便用户随时进行网络拓扑信息的收集，从而进行设备的管理与监控。

可以使用下面的命令手动进行拓扑信息的收集。

请在用户视图下进行下列配置。

表2-11 启动拓扑信息的收集过程

操作	命令
启动拓扑信息的收集过程	**ntdp explore**

2.3.8 NTDP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后 NTDP 的运行情况。用户可以通过查看显示信息验证配置的效果。

表2-12 NTDP 显示和调试

操作	命令
显示全局 NTDP 信息	**display ntdp**
显示 NTDP 收集到的设备信息	**display ntdp device-list** [**verbose**]

在使用 **display ntdp device-list** 命令时，如果不带 **verbose** 参数，将显示 NTDP 收集到的设备列表信息；如果带 **verbose** 参数，将显示 NTDP 收集到的设备的详细信息。

显示维护命令的显示信息及说明请参见命令手册。

2.4 集群配置

2.4.1 集群简介

本节主要介绍与集群管理相关的配置，包括集群的使能与建立、管理设备公网 IP 地址的配置、集群成员的加入/删除以及握手间隔的配置等。

每个集群必须指定一个（而且只能指定一个）管理设备。由于一个集群只能有一个管理设备，因此在建立集群时，首先需要确定一个管理设备。外部网络对集群内部各成员的访问、配置、管理、监控等都需要经过管理设备，管理设备是访问集群成员的出入口。管理设备识别并控制集群中的所有成员设备，不管这些成员设备分布在网络的什么地方，也不管他们是如何相连的。同时在集群建立过程中，为了给用户提供可供参考的候选设备信息以及网络拓扑结构信息，管理设备将负责收集所有成员设备和候选设备的拓扑信息。

管理设备通过收集 NDP/NTDP 信息，了解网络的拓扑结构，从而进行设备的管理与监控。

在各项配置任务中，必须先使能集群功能，才能配置其它任务。

集群主要配置包括：

- 使能/禁止集群功能
- 进入集群视图
- 配置集群 IP 地址池
- 配置集群名称
- 集群成员的加入与删除
- 自动建立集群
- 配置交换机的有效保留时间

- 配置握手报文定时发送的时间间隔
- 配置集群内部公用的服务器及网管、日志主机
- 成员访问

📖 **说明：**

管理设备上需要启动集群功能，并且配置集群的参数。而成员设备和候选设备上只需要启动集群功能，从而接受管理设备的管理。

2.4.2 使能/禁止集群功能

在使用集群功能前，必须先使能交换机的集群功能。

可以使用下面的命令来使能/禁止当前交换机的集群功能。

请在系统视图下进行下列配置。

表2-13 使能/禁止集群功能

操作	命令
使能集群功能	**cluster enable**
禁止集群功能	**undo cluster enable**

以上命令可以在任何支持集群功能的交换机上执行。如果在管理设备上执行 **undo cluster enable** 命令，将删除集群以及集群的成员，中止交换机成为管理设备的功能，同时交换机的集群功能将被禁止。如果在成员设备上执行 **undo cluster enable** 命令，交换机将从集群中退出，集群功能被禁止。如果在非集群内的交换机上执行 **undo cluster enable** 命令，交换机的集群功能将被禁止。

缺省情况下，交换机上的集群功能处于启动状态。

2.4.3 进入集群视图

要进行集群参数配置前必须首先进入集群视图。

请在系统视图下进行下列配置。

表2-14 进入集群视图

操作	命令
进入集群视图	**cluster**

2.4.4 配置集群 IP 地址池

在建立集群前，用户需首先设置集群中成员设备使用的私有 IP 地址范围，当候选设备加入时，管理设备动态分配一个能够在集群范围内使用的私有 IP 地址，并下发给候选设备，用于集群内部的通信，以实现管理设备对成员设备的管理和维护。

可以使用下面的命令在管理设备上配置集群的 IP 地址池。

请在集群视图下进行下列配置。

表2-15 配置集群 IP 地址池

操作	命令
配置集群 IP 地址范围	**ip-pool** *administrator-ip-address { ip-mask | ip-mask-length}*
恢复集群缺省的 IP 地址范围	**undo ip-pool**

在建立集群之前，用户必须首先配置 IP 地址池。

需要注意的是，只能当集群还没有建立时才能进行本配置，并且只能在管理设备上进行本配置。如果集群已经建立，则系统不允许修改 IP 地址范围。

2.4.5 配置集群名称

每个集群都有自己的名称。

可以通过以下命令在确定为管理设备的交换机上配置集群名称，同时该交换机也正式成为管理设备。

请在集群视图下进行下列配置。

表2-16 配置管理设备及集群名称

操作	命令
配置管理设备及集群名称	**build** *name*
删除集群中的所有成员并将管理设备配置为候选设备	**undo build**

需要注意的是，**build** 命令只能在确定为管理设备的交换机使用，该交换机不能是其它集群的成员设备。如果当前交换机已经配置为某个集群的成员设备，则该交换机不能进行本配置。如果交换机已经是某个集群的管理设备，本配置将使用配置的集群名称更改原来的集群名称。

缺省情况下，交换机不是管理设备，并且未指定集群名称。

2.4.6 集群成员的加入与删除

用户可以手工指定要加入集群中的候选设备，也可以手工删除集群中指定的成员设备。

可以使用下面的命令来增加一个集群成员设备或者删除一个集群成员设备。

请在集群视图下进行下列配置。

表2-17 集群成员的加入与删除

操作	命令
集群成员的加入	**add-member** [*member-num*] **mac-address** *H-H-H* [**password** *password*]
集群成员的删除	**delete-member** *member-num*

需要注意的是，集群成员的加入/删除操作必须在管理设备上进行，否则将返回错误提示信息。

上述命令中 *member-num*、**mac-address** *H-H-H*、**password** *password* 参数是待加入成员设备的成员编号、MAC 地址和该交换机进入系统视图时的密码。在向集群加入新成员时，可以不指定成员编号，管理设备会自动为新加入的成员设备指定可用的成员编号。当成员设备加入集群后，它进入系统视图的密码将被自动修改为管理设备进入系统视图的密码。

2.4.7 自动建立集群

除了手工向集群加入成员的方法外，系统给用户提供了一种自动建立集群的功能。用户只要在管理设备上使用以下命令，即可根据提示的信息一步步创建集群。

在自动创建集群的过程中，系统首先提示输入集群名称，接着将列出指定的跳数范围内发现的所有候选设备的列表，提示用户确认是否向集群加入这些交换机。在用户确认后，系统将把所有列出的候选设备自动加入到创建的集群中。

在自动创建过程中，允许用户输入<CTRL+C>取消当前操作，并且退出自动创建过程。这个操作只是停止加入新的交换机，已经加入集群的交换机将保留在集群中。

请在集群视图下进行下列配置。

表2-18 自动建立集群

操作	命令
自动建立集群	**auto-build** [**recover**]

需要注意的是，用户只能在管理设备上才能执行自动创建集群的操作。

2.4.8 配置交换机的有效保留时间

集群建立后，由于网络或交换机重启等原因，可能会造成通讯故障。如果故障时间超出配置的交换机有效保留时间，成员的状态将显示为“down”。当通讯得到恢复时，相应的成员设备要重新进行加入集群（成员的重新加入过程将自动进行）；如果故障时间没有超出用户规定的有效保留时间，则不需要重新进行成员加入，成员始终为正常状态。

可以使用下面的命令在管理设备上配置交换机的有效保留时间。

请在集群视图下进行下列配置。

表2-19 配置交换机的有效保留时间

操作	命令
配置交换机的有效保留时间	**holdtime** *seconds*
恢复交换机的有效保留时间为缺省值	**undo holdtime**

需要注意的是，本命令仅在管理设备上执行，由管理设备把时间值传播给其它的成员设备。

缺省情况下，交换机的有效保留时间为 60 秒。

2.4.9 配置握手报文定时发送的时间间隔

在集群内部，成员设备与管理设备的实时通信是通过握手报文来维系的。通过成员设备和管理设备之间的定时握手，管理设备可以监视集群内各成员的状态以及链路状态。

成员设备加入集群后，就开始定时和管理设备握手。握手由成员设备主动发起，定时发送。无论是管理设备还是成员设备，如果收到定时握手报文，则认为当前的通信状态是正常的。

成员设备如果连续 3 次收不到管理设备的握手应答报文，则认为和管理设备间的通讯故障；同样，如果管理设备连续 3 次收不到成员设备的握手请求报文，则认为和该成员设备间的通讯故障。

同时，如果成员设备发现拓扑改变时，它将通过握手报文上报管理设备来处理。

可以使用下面的命令在管理设备上配置握手报文定时发送的时间间隔。

请在集群视图下进行下列配置。

表2-20 配置握手报文定时发送的时间间隔

操作	命令
配置握手报文定时发送的时间间隔	**timer** *interval*
恢复握手报文定时发送的时间间隔为缺省值	**undo timer**

需要注意的是，本命令仅在管理设备上执行，由管理设备把时间值传播给其它的成员设备。

缺省情况下，握手报文定时发送的时间间隔为 10 秒。

2.4.10 配置成员设备的远程控制

如果由于某些错误的配置造成成员设备的故障时，用户可以利用管理设备的远程控制功能对成员设备进行远程控制（例如，删除启动配置文件并重启成员设备），以达到恢复管理设备和成员设备之间的正常通信的目的。

一般情况下，集群的报文只能在 VLAN1 中转发。如果用户在成员设备上进行了错误配置，比如将成员设备上与管理设备相连的端口设置为属于 VLAN2 的端口，会造成管理设备和成员设备无法进行通信。用户可以通过在管理设备上配置 VLAN 检查功能解决上述问题。在进行此项配置后，管理设备向成员设备发送的集群报文中将会携带这个配置信息。成员设备收到这种报文后，如果接收报文的端口不属于 VLAN1，成员设备会自动将该端口加入到 VLAN1 中，保证和管理设备的正常通信。

可以使用下面的命令进行上述的配置。

请在集群视图下进行下列配置。

表2-21 配置成员设备的远程控制

操作	命令
重启成员设备	**reboot member** { *member-num* | **mac-address** *H-H-H* } [**eraseflash**]
配置集群内部通信进行 VLAN 检查设置	**port-tagged vlan** *vlanid*
配置集群内部通信不进行 VLAN 检查设置	**undo port-tagged**

需要注意的是，以上命令仅在管理设备上执行。

在使用 **reboot member** 命令时，用户可以通过 **eraseflash** 参数来控制在成员设备重启时是否删除启动时的配置文件。

2.4.11 配置集群内部公用的服务器及网管、日志主机

在集群建立后，用户可以在管理设备上为集群统一配置服务器、网管主机和日志主机。

集群成员设备将通过管理设备来访问配置的服务器。

集群内部成员设备的所有日志信息都将输出到配置的日志主机上：在集群成员设备输出日志信息时，日志信息直接发送给管理设备，然后管理设备对这些日志信息进行地址转换，把成员设备的日志报文发送到为集群配置的日志主机上。同样，集群成员设备的所有 trap 报文都输出到为集群配置的网管主机上。

可以使用下面的命令在管理设备上配置集群内部公用的服务器及网管、日志主机。

请在集群视图下进行下列配置。

表2-22 配置集群内部公用的服务器及网管、日志主机

操作	命令
配置集群内部公用的 FTP Server	**ftp-server** *ip-address*
删除集群内部公用的 FTP Server	**undo ftp-server**
配置集群内部公用的 TFTP Server	**tftp-server** *ip-address*
删除集群内部公用的 TFTP Server	**undo tftp-server**
配置集群内部公用的日志主机	**logging-host** ip-address
删除集群内部公用的日志主机	**undo logging-host**
配置集群内部公用的网管主机	**snmp-host** ip-address
删除集群内部公用的网管主机	**undo snmp-host**

需要注意的是，以上命令仅在管理设备上配置。

2.4.12 成员访问

在正确配置了 NDP、NTDP、集群以后，用户可以通过管理设备对集群中的成员进行管理。在管理设备上，用户可以切换到指定的成员设备视图下对该成员设备进行配置管理；也可以从成员设备视图切换回管理设备的视图对管理设备进行配置。

从管理设备视图切换到成员设备视图时，需要鉴权。如果鉴权通过，则允许切换；如果成员设备的用户密码与管理设备的不同，则拒绝切换。从管理设备视图切换到成员设备视图时，继承管理设备视图上的用户级别。例如：切换前管理设备处于用户视图，切换后在成员设备上同样是用户视图。

从成员设备视图切换回管理设备视图时，也需要鉴权，鉴权通过后，管理设备将自动进入用户视图。

请在用户视图下进行下列配置。

表2-23 成员访问

操作	命令
成员访问	**cluster switch-to** { *member-num* | **mac-address** *H-H-H* | **administrator** }

需要注意的是，在管理设备上使用此命令时，如果指定的成员号 *member-num* 不存在，系统将显示出错信息。结束切换只需输入 **quit** 即可。

2.4.13 集群显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后集群的运行情况。用户可以通过查看显示信息验证配置的效果。

表2-24 集群显示和调试

操作	命令
显示集群状态和统计信息	**display cluster**
显示候选设备信息	**display cluster candidates** [**mac-address** *H-H-H* | **verbose**]
显示集群成员信息	**display cluster members** [*member-num* | **verbose**]

显示维护命令的显示信息及说明请参见命令手册。

2.5 HGMP V2 配置举例

1. 组网需求

三台交换机构成一个集群，管理设备管理两台成员设备。管理设备通过端口 GigabitEthernet0/1 和端口 GigabitEthernet0/2 挂了两台成员设备。管理设备通过端口 GigabitEthernet0/4 接入到外部网络，GigabitEthernet0/4 属于 VLAN2，VLAN2 的接口 IP 地址为 163.172.55.1，整个集群使用相同的 FTP server、TFTP server，FTP server、TFTP server 的 IP 地址为 63.172.55.1，网管工作站及日志主机的 IP 地址为 69.172.55.4。

2. 组网图

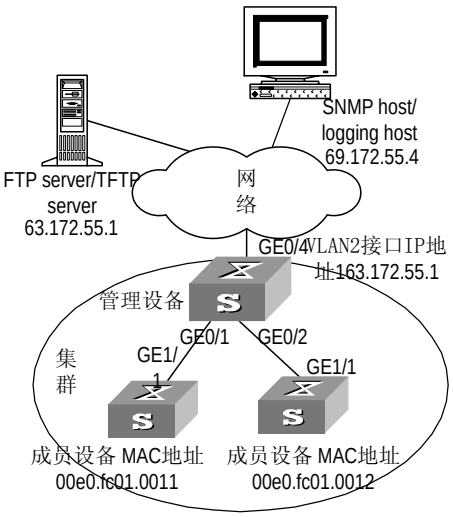


图2-3 HGMP 集群管理组网图

3. 配置步骤

(1) 配置管理设备

启动设备上的 NDP 和端口 GE0/1、GE0/2 上的 NDP。

[Quidway] ndp enable

[Quidway] interface gigabitethernet 0/1

[Quidway-GigabitEthernet0/1] ndp enable

[Quidway-GigabitEthernet0/1] interface gigabitethernet 0/2

[Quidway- GigabitEthernet0/2] ndp enable

配置 NDP 信息的有效保留时间为 200 秒。

[Quidway] ndp timer aging 200

配置 NDP 报文发送的时间间隔为 70 秒。

[Quidway] ndp timer hello 70

启动设备上的 NTDP 和端口 GE0/1、GE0/2 上的 NTDP。

[Quidway] ntdp enable

[Quidway] interface gigabitethernet 0/1

[Quidway-GigabitEthernet0/1] ntdp enable

[Quidway-GigabitEthernet0/1] interface gigabitethernet 0/2

[Quidway-GigabitEthernet0/2] ntdp enable

配置拓扑收集范围为 2 跳

[Quidway] ntdp hop 2

配置被收集设备转发拓扑收集请求的延迟时间为 150ms。

[Quidway] ntdp timer hop-delay 150

配置被收集设备的端口转发拓扑收集请求的延迟时间为 15ms。

[Quidway] ntdp timer port-delay 15

配置定时拓扑收集的时间间隔为 3 分钟。

[Quidway] ntdp timer 3

启动集群功能。

[Quidway] cluster enable

进入集群视图。

[Quidway] cluster

[Quidway-cluster]

配置集群内部使用的 IP 地址池，起始地址为 172.16.0.1，有 8 个地址

[Quidway-cluster] ip-pool 172.16.0.1 255.255.255.248

配置集群名字，建立集群。

[Quidway-cluster] build huawei

[huawei_0. Quidway-cluster]

将下挂的两个交换机加入到集群中。

[huawei_0. Quidway-cluster] add-member 1 mac-address 00e0-fc01-0011

[huawei_0. Quidway-cluster] add-member 17 mac-address 00e0-fc01-0012

配置成员设备信息的保留时间为 100 秒。

[huawei_0. Quidway-cluster] holdtime 100

配置握手报文定时发送的时间间隔为 10 秒。

[huawei_0. Quidway-cluster] timer 10

配置集群内部公用的 FTP Server、TFTP Server、Logging host 及 SNMP host。

[huawei_0. Quidway-cluster] ftp-server 63.172.55.1

[huawei_0. Quidway-cluster] tftp-server 63.172.55.1

[huawei_0. Quidway-cluster] logging-host 69.172.55.4

[huawei_0. Quidway-cluster] snmp-host 69.172.55.4

(2) 配置成员设备（以一台成员设备为例）

启动设备上的 NDP 和端口 GigabitEthernet1/1 上的 NDP。

[Quidway] ndp enable

[Quidway] interface gigabitethernet 1/1

[Quidway-GigabitEthernet1/1] ndp enable

启动设备上的 NTDP 和端口 Ethernet1/1 上的 NTDP。

[Quidway] ntdp enable

[Quidway] interface gigabitethernet 1/1

[Quidway-GigabitEthernet1/1] ntdp enable

启动集群功能。

[Quidway] cluster enable

📖 **说明：**

在进行了上述配置之后，用户只要在管理设备上通过命令 **cluster switch-to** { *member-num* | **mac-address** *H-H-H* }切换到成员设备配置视图就可以对成员设备进行维护管理，通过命令 **cluster switch-to administrator** 切换回管理设备配置视图。在管理设备上用户还可以通过命令 **reboot member** { *member-num* | **mac-address** *H.H.H* } [**eraseflash**]对成员设备进行重启操作。关于这些配置操作的具体描述请参见本章前面的相关配置描述。

目 录

第1章 MSTP 配置

1.1 MSTP 简介

MSTP（Multiple Spanning Tree Protocol）是多生成树协议的英文缩写，该协议兼容 STP（Spanning Tree Protocol）和 RSTP（Rapid Spanning Tree Protocol）。

STP 不能快速迁移。即使是在点对点链路或边缘端口，也必须等待 2 倍的 Forward delay 的时间延迟，端口才能迁移到转发状态。

RSTP 可以快速收敛，但是和 STP 一样存在以下缺陷：局域网内所有网桥共享一棵生成树，不能按 VLAN 阻塞冗余链路，所有 VLAN 的报文都沿着一棵生成树进行转发。

关于 STP、RSTP 相关的描述可以参见 RSTP 配置章节的描述。

MSTP 可以弥补 STP 和 RSTP 的缺陷，它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

MSTP 设置 VLAN 映射表（即 VLAN 和生成树的对应关系表）把 VLAN 和生成树联系起来。同时它把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。MSTP 将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

1.1.1 MSTP 的几个概念

在 图 1-1中有四个MST域，每个域都由四台交换机构成。交换机都运行MSTP。下面将结合图形解释MSTP的几个概念。

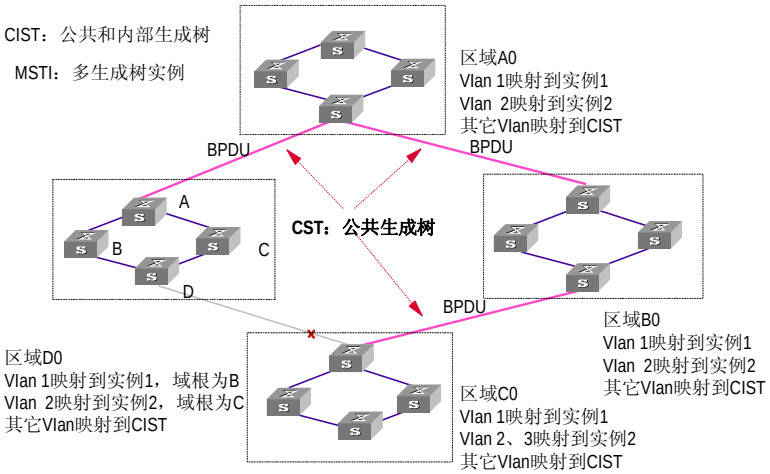


图1-1 MSTP 的基本概念示意图

1. MST 域

MST域（Multiple Spanning Tree Regions）：多生成树域，是由交换网络中的多台交换机以及它们之间的网段所构成，这些交换机都启动了MSTP、具有相同域名，具有相同VLAN到生成树映射配置，具有相同MSTP修订级别配置，并且物理上直接相连。一个交换网络可以存在多个MST域。用户可以通过MSTP配置命令把多台交换机划分在同一个MST域内。例如 图 1-1中的区域A0，域内所有交换机都有相同的MST域配置：域名相同，VLAN与生成树的映射关系相同（VLAN1 映射到生成树实例 1，VLAN2 映射到生成树实例 2，其余VLAN映射到CIST），相同的MSTP修订级别（此配置在图中没有体现）。

2. VLAN 映射表

MST域的一个属性，是描述VLAN和生成树实例关系的对应表。例如 图 1-1中，域A0 的VLAN映射表就是：VLAN 1 映射到生成树实例 1，VLAN2 映射到生成树实例 2，其余VLAN映射到CIST。

3. IST

IST（Internal Spanning Tree）：内部生成树，是MSTP域内的一棵生成树，它和CST（Common Spanning Tree）共同构成整台交换机网络的生成树CIST（Common and Internal Spanning Tree）。IST是CIST在一个MST域中的片段。例如 图 1-1中CIST在每个MST域内都有一个片段，这个片段就是各个域内的IST。

4. CST

CST（Common Spanning Tree）：公共生成树连接交换网络内所有MST域的单生成树。如果把每个MST域看作是一个“交换机”，CST就是这些“交换机”通过STP协议、RSTP协议计算生成的一棵生成树。例如 图 1-1中红色线条描绘的就是CST。

5. CIST

CIST（Common and Internal Spanning Tree）：公共和内部生成树，由IST和CST共同构成，是连接一个交换网络内所有交换机的单生成树。例如 图 1-1中，每个域内的IST加上域间的CST就构成整个网络的CIST。

6. MSTI

MSTI（Multiple Spanning Tree Instance）：多生成树实例，一个MST域内可以通过MSTP生成多棵生成树，各棵生成树之间彼此独立。每棵生成树都称为一个MSTI，即多生成树实例。例如 图 1-1中，每个域内可以存在多棵生成树，每棵生成树和相应的VLAN对应。这些生成树就被称为MSTI。

7. 域根

MST域内IST和MSTI的树根就是域根。MST域内各棵生成树的拓扑不同，域根也可能不同。例如 图 1-1中，区域D0 中，生成树实例 1 的域根为交换机B，生成树实例 2 的域根为交换机C。

8. Common Root Bridge

CIST的根交换机就是Common Root Bridge，即总根。例如 图 1-1中，总根为区域A0 内的某台交换机。

9. 域边缘端口

域边缘端口是指位于MST域的边缘，连接不同MST域、或者连接MST域和运行STP的区域、或者连接MST域和运行RSTP的区域的端口。在进行MSTP计算的时候，域边缘端口在MST实例上的角色和CIST实例的角色保持一致，即如果边缘端口在CIST实例上的角色是master端口，则它在域内所有MST实例上的角色也是master端口。例如 图 1-1中，如果区域A0 的一台交换机和区域D0 的一台交换机的第一个端口相连，整个交换网络的总根位于A0 内，则区域D0 的这台交换机上的第一个端口就是区域D0 的域边缘端口。

10. 端口的角色

在 MSTP 的计算过程中，端口的角色有指定端口、根端口、Master 端口、Alternate 端口、Backup 端口等。

- 根端口是负责向树根方向转发数据的端口；
- 指定端口是负责向下游网段或交换机转发数据的端口；
- Master 端口位于整个域到 Common Root Bridge 的最短路径上，它是连接域到 Common Root Bridge 的端口；
- Alternate 端口是 Master 端口的备份端口。如果 Master 端口被阻塞后，Alternate 端口将成为新的 Master 端口；
- 当同一台交换机的两个端口互相连接时就存在一个环路，此时交换机会将其中一个端口阻塞，Backup 端口是阻塞的那个端口。

端口在不同的生成树实例中可以担任不同的角色。

请参见下面的图示理解以上的各个概念。图 1-2中，交换机A、B、C、D构成一个MST域。A交换机的端口 1、2 向总根方向连接，交换机C的端口 5 和端口 6 构成了环路，交换机D的端口 3、4 则向下连接其他的MST域。

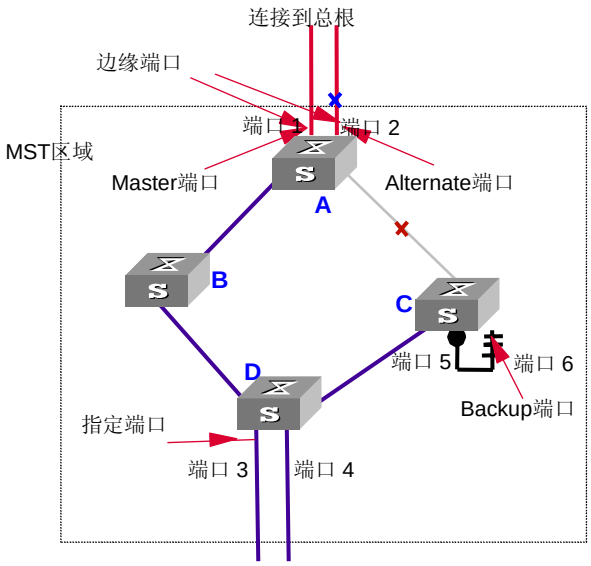


图1-2 端口角色示意图

1.1.2 MSTP 的基本原理

MSTP 将整个二层网络划分为多个 MST 域，各个域之间通过计算生成 CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。其中实例 0 被称为 IST，其他的多生成树实例为 MSTI。MSTP 同 RSTP 一样，使用配置消息进行生成树的计算，只是配置消息中携带的是交换机上 MSTP 的配置信息。

1. CIST 生成树的计算

通过“配置消息”的比较在整个网络中选择一个优先级最高的交换机作为 CIST 的树根。在每个 MST 域内 MSTP 通过计算生成 IST；同时 MSTP 将每个 MST 域作为单台交换机对待，通过计算在域间生成 CST。CST 和 IST 构成了整台交换机网络中连接所有交换机的 CIST。

2. MSTI 的计算

在 MST 域内，MSTP 根据 VLAN 和生成树实例的映射关系，针对不同的 VLAN 生成不同的生成树实例，即 MSTI。每棵生成树独立进行计算，计算过程与 RSTP 计算生成树的过程类似，下面对单个生成树的计算过程进行举例介绍。

生成树的基本原理是，通过在交换机之间传递一种特殊的协议报文（在 IEEE 802.1D 中这种协议报文被称为“配置消息”）来确定网络的拓扑结构。配置消息中包含了足够的信息来保证交换机完成生成树计算。

配置消息中主要包括以下内容：

(1) 树根的 ID：由树根的优先级和 MAC 地址组合而成；

(2) 到树根的最短路径开销；

(3) 指定交换机的 ID：由指定交换机的优先级和 MAC 地址组合而成；

(4) 指定端口的 ID：由指定端口的优先级和端口编号组成；

(5) 配置消息的生存期：MessageAge；

(6) 配置消息的最大生存期：MaxAge；

(7) 配置消息发送的周期：HelloTime；

(8) 端口状态迁移的延时：ForwardDelay。

指定端口和指定交换机的含义，请参见下面的说明：

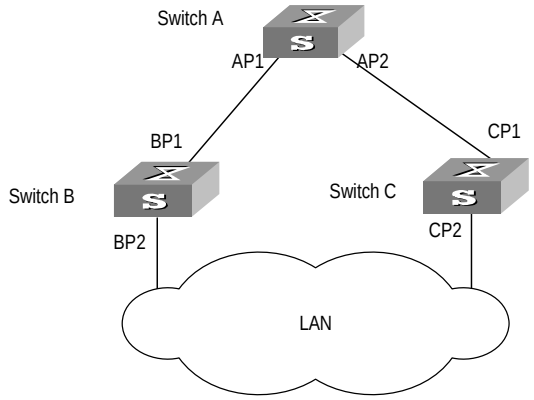


图1-3 指定交换机和指定端口示意图

对一台交换机而言，指定交换机就是与本机直接相连并且负责向本机转发数据包的交换机，指定端口就是指定交换机向本机转发数据的端口；对于一个局域网而言，指定交换机就是负责向这个网段转发数据包的交换机，指定端口就是指定交换机向这个网段转发数据的端口。如 图 1-3所示，AP1、AP2、BP1、BP2、CP1、CP2 分别表示Switch A、Switch B、Switch C的端口，Switch A通过端口AP1 向Switch B转发数据，则Switch B的指定交换机就是Switch A，指定端口就是Switch A的端口AP1；与局域网LAN相连的有两台交换机：Switch B和Switch C，如果Switch B负责向LAN转发数据包，则LAN的指定交换机就是Switch B，指定端口就是Switch B的BP2。

- 生成树协议算法实现的具体过程：

下面结合例子说明生成树协议算法实现的计算过程。

具体的组网如 图 1-4所示：

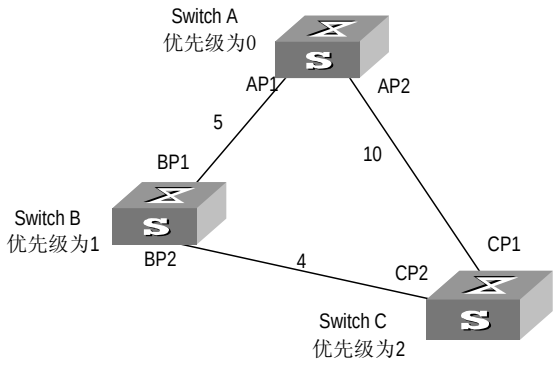


图1-4 举例中的以太网交换机组网图

为描述方便，在举例中仅给出配置消息的前四项：树根 ID（以以太网交换机的优先级表示），根路径开销，指定交换机 ID（以以太网交换机的优先级表示），指定端口 ID（以端口号表示）。如上图所示，Switch A 的优先级为 0，

Switch B 的优先级为 1，Switch C 的优先级为 2，各个链路的路径开销如图中所示，分别为 5、10、4。

(1) 初始状态

各台交换机的各个端口在初始时会生成以自己为根的配置消息，根路径开销为 0，指定交换机 ID 为自身交换机 ID，指定端口为本端口。

Switch A：

端口 AP1 配置消息：{0，0，0，AP1}

端口 AP2 配置消息：{0，0，0，AP2}

Switch B：

端口 BP1 配置消息：{1，0，1，BP1}

端口 BP2 配置消息：{1，0，1，BP2}

Switch C：

端口 CP2 配置消息：{2，0，2，CP2}

端口 CP1 配置消息：{2，0，2，CP1}

(2) 选出最优配置消息

各台交换机都向外发送自己的配置消息。当某个端口收到比自身的配置消息优先级低的配置消息时，交换机会将接收到的配置消息丢弃，对该端口的配置消息不作任何处理。当端口收到比本端口配置消息优先级高的配置消息的时候，交换机就用接收到的配置消息中的内容替换该端口的配置消息中的内容。然后以太网交换机将该端口的配置消息和交换机上的其它端口的配置消息进行比较，选出最优的配置消息

配置消息的比较原则是：

- 树根 ID 较小的配置消息优先级高；
- 若树根 ID 相同，则比较根路径开销，比较方法为：用配置消息中的根路径开销加上本端口对应的路径开销之和（设为 S），则 S 较小的配置消息优先级较高；
- 若根路径开销也相同，则依次比较指定交换机 ID、指定端口 ID、接收该配置消息的端口 ID 等。

为便于表述，本例中假设只需比较树根 ID 就可以选出最优配置消息。

(3) 确定根端口，并阻塞冗余链路，然后更新指定端口的配置消息

交换机接收最优配置消息的那个端口定为根端口，端口配置消息不作改变；其它端口中，如果某端口的配置消息在过程“选出最优配置消息”中更新过，则交换机将此端口阻塞，端口配置消息不变，此端口将不再转发数据，并且只接收但不发送配置消息；如果某端口的配置消息在过程“选出最优配置消息”中没有更新，则交换机就将其定为指定端口，配置消息要作如下改变：树根 ID 替换为根端口的配置消息的树根 ID；根路径开销替换为根端口的配置消息的根路径开销加上根端口对应的路径开销；指定交换机 ID 替换为自身交换机的 ID；指定端口 ID 替换为自身端口 ID。

例子中各台交换机的比较过程如下：

Switch A：

端口 AP1 收到 Switch B 的配置消息，Switch A 发现本端口的配置消息优先级高于接收到的配置消息的优先级，就把接收到的配置消息丢弃。端口 AP2 的配置消息处理过程与端口 AP1 类似。Switch A 发现自己各个端口的配置消息中树根和指定交换机都是自己，则认为自己是树根，各个端口的配置消息都不作任何修改，以后周期性的向外发送配置消息。此时两个端口的配置消息如下：

端口 AP1 配置消息：{0，0，0，AP1}。

端口 AP2 配置消息：{0，0，0，AP2}。

Switch B：

端口 BP1 收到来自 Switch A 的配置消息，经过比较后 Switch B 发现接收到的配置消息的优先级比端口 BP1 的配置消息的优先级高，于是更新端口 BP1 的配置消息。

端口 BP2 收到来自 Switch C 的配置消息，Switch B 发现该端口的配置消息优先级高于接收到的配置消息的优先级，就把接收到的配置消息丢弃。

则此时各个端口的配置消息如下：端口 BP1 配置消息：{0，0，0，AP1}，端口 BP2 配置消息：{1，0，1，BP2}。

Switch B 对各个端口的配置消息进行比较，选出端口 BP1 的配置消息为最优配置消息，然后将端口 BP1 定为根端口，整台交换机各个端口的配置消息都进行如下更新：

根端口 BP1 配置消息不作改变：{0，0，0，AP1}。端口 BP2 配置消息中，树根 ID 更新为最优配置消息中的树根 ID，根路径开销更新为 5，指定交换机 ID 更新为本交换机 ID，指定端口 ID 更新为本端口 ID，配置消息变为：{0，5，1，BP2}。

然后 Switch B 各个指定端口周期性向外发送自己的配置消息。

Switch C：

端口 CP2 先会收到来自 Switch B 端口 BP2 更新前的配置消息{1，0，1，BP2}，Switch C 触发更新过程，更新后的配置消息如下：{1，0，1，BP2}。

端口 CP1 收到来自 Switch A 的配置消息{0，0，0，AP2}后 Switch C 也触发更新过程，更新后的配置消息如下：{0，0，0，AP2}。

经过比较，端口 CP1 的配置消息被选为最优的配置消息，端口 CP1 就被定位根端口，它的配置消息就不作改变；而端口 CP2 就会被阻塞，端口配置消息也不作改变，同时该端口不接收从 Switch B 转发的数据（不包括 STP 的协议报文），直到新的情况发生触发生成树的重新计算，比如从 Switch B 到 Switch C 的链路 down 掉，或者端口收到更优的配置消息。

接着端口 CP2 会收到 Switch B 更新后的配置消息{0，5，1，BP2}，由于收到的配置消息比原配置消息优，则 Switch C 触发更新过程，更新后的配置消息为：{0，5，1，BP2}。

同时端口 CP1 收到来自 Switch A 配置消息，比较后 Switch C 不会触发更新过程，配置消息仍然为：{0，0，0，AP2}。

经过比较，端口 CP2 的配置消息被选为最优的配置消息，端口 CP2 就被定为根端口，它的配置消息就不作改变，而端口 CP1 就被阻塞，端口配置消息不变，同时不接收从 Switch A 转发的数据，直到新的情况触发生成树的计算，比如从 Switch B 到 Switch C 的链路 down 掉。

此时生成树就被确定下来，形状如 图 1-5，树根为Switch A：

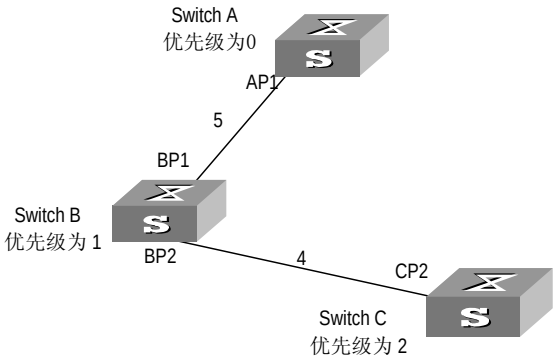


图1-5 最终稳定的生成树

本例为了描述方便，简化了很多计算、操作内容（比如树根 ID 和指定交换机 ID 在实际运算的过程中应该是由交换机的优先级和 MAC 地址共同组成的，指定端口 ID 则是由端口优先级和端口 MAC 地址共同构成；在配置消息的更新

过程中，除了前四项会改变以外，其它配置消息也会按照一定的原则进行改变），但计算过程基本如此。

- 生成树协议的配置消息传递机制：

当网络初始化时，所有的交换机都将自己作为树根。交换机的指定端口以 HelloTime 为周期，定时发送本端口的配置消息；接收到配置消息的端口如果是根端口，则交换机将配置消息中携带的 MessageAge 按照一定的原则递增，并启动定时器为这条配置消息计时。如果某条路径发生故障，则这条路径上的根端口不会再收到新的配置消息，旧的配置消息将会因为超时而被丢弃，从而引发生成树的重新计算，得到一条新的通路替代发生故障的链路，恢复网络连通性。

不过，重新计算得到的新配置消息不会立刻就传遍整个网络，因此那些没有发现网络拓扑已经改变的旧的根端口和指定端口仍旧会按照原来的路径继续转发数据，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的路径回环。为此 STP 采用了一种状态迁移的机制，根端口和指定端口重新开始数据转发之前要经历一个中间状态，中间状态经过 Forward Delay 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。

这样一个 VLAN 的报文将沿着如下路径进行转发：在 MST 域内将沿着其对应的 MSTI 转发，在域间则沿着 CST 转发。

1.1.3 MSTP 在交换机上的实现

MSTP 同时兼容 STP、RSTP。STP、RSTP 两种协议报文都可以被运行 MSTP 的交换机识别并应用于生成树计算。Quidway 系列以太网交换机除了提供 MSTP 的基本功能外，还从用户的角度出发，提供了许多便于管理的特殊功能：根桥保持、根桥备份、ROOT 保护功能、BPDU 保护功能、环路保护功能。MSTP 支持接口板的热插拔，同时支持主控板与备板的倒换。

1.2 MSTP 配置

MSTP 配置包括：

- 配置交换机的 MST 域
- 指定交换机为根交换机或备份根交换机
- 配置 MSTP 的工作模式
- 配置交换机的 Bridge 优先级
- 配置 MST 域的最大跳数

- 配置交换网络的网络直径
- 配置交换机的时间参数
- 配置端口的最大发送速率
- 配置端口是否可以作为 EdgePort
- 配置端口的 Path Cost
- 配置端口的优先级
- 配置端口是否与点对点链路相连
- 配置端口的 mCheck 变量
- 配置交换机的保护功能
- 开启设备 MSTP 特性
- 开启端口 MSTP 特性

只有开启设备 MSTP 特性后其他配置才能生效。在启动 MSTP 之前，可以配置设备或以太网端口的相关参数；启动 MSTP 后，这些参数将生效；MSTP 关闭后，这些配置参数仍被保留；当 MSTP 重新启动后，这些参数仍将生效。未生效的域参数可以使用 **check region-configuration** 命令显示；在 MSTP 未启动前配置的其他参数可以使用 **display current-configuration** 命令来显示；启动后的 MSTP 参数可以使用相关的 **display** 命令显示，可以参考本章的“MSTP 显示和调试”章节。

📖 **说明：**

当 GVRP 和 MSTP 同时在交换机上启动时，GVRP 报文将沿着生成树实例 CIST 进行传播。因此在 GVRP 和 MSTP 同时在交换机上启动的情况下，如果用户希望通过 GVRP 在网络中发布某个 VLAN，则用户在配置 MSTP 的 VLAN 映射表时要保证把这个 VLAN 映射到 CIST 上。
CIST 即生成树实例 0。

1.2.1 配置交换机的 MST 域

交换机属于哪个 MST 域由域名、VLAN 映射表、MSTP 修订级别配置决定。用户可以通过下面的配置过程将当前交换机划分在一个特定的 MST 域内。

1. 进入 MST 域视图

请在系统视图下进行下列配置。

表1-1 进入 MST 域视图

操作	命令
进入 MST 域视图	**stp region-configuration**
将 MST 域的三个配置恢复为缺省值	**undo stp region-configuration**

2. 配置 MST 域的参数

请在 MST 域视图下进行下列配置。

表1-2 配置交换机的 MST 域

操作	命令
配置 MST 域的域名（MST 域视图）	**region-name** *name*
配置 MST 域的域名为缺省值（MST 域视图）	**undo region-name**
配置 VLAN 映射表（MST 域视图）	**instance** *instance-id* **vlan** *vlan-list*
配置 VLAN 映射表为缺省值（MST 域视图）	**undo instance**
配置 MST 域的 MSTP 修订级别（MST 域视图）	**revision-level** *level*
配置 MST 域的修订级别为缺省值（MST 域视图）	**undo revision-level**

在一个 MST 域内最多可以包含 17 棵生成树实例，其中实例 0 为 IST，实例 1～16 为 MSTI（多生成树实例）。用户在交换机上对 MST 域作了以上配置，就把当前交换机划分到了一个特定的 MST 域内。需要注意的是，只有两台交换机上配置的 MST 域的域名相同、MST 域内配置的所有生成树实例对应的 VLAN 映射表完全相同、MST 域的修订级别相同，这两台交换机才属于同一个 MST 域。

用户在配置 MST 域的相关参数，特别是配置 VLAN 映射表时，会引起 MSTP 重新计算生成树，从而引起网络拓扑振荡。为了减少这种由于配置引起的振荡，MSTP 在处理用户关于域的相关配置时，并不会马上触发生成树重新计算，而是在满足下列条件之一的情况下，这些域的配置才会真正的生效：

- 用户使用命令 **active region-configuration** 手工激活配置的 MST 域相关参数
- 用户使用命令 **stp enable** 使能 MSTP

缺省情况下，MST 域的域名等于交换机的第一个 MAC 地址，MST 域内所有的 VLAN 都映射到生成树实例 0，MSTP 域的修订级别为 0。用户可以在系统

视图下使用命令 **undo stp region-configuration** 将 MST 域的三个配置恢复为缺省值。

3. 激活 MST 域的配置，并退出 MST 域视图

请在 MST 域视图下进行下列配置。

表1-3 激活 MST 域的配置，并退出 MST 域视图

操作	命令
显示正在修改的 MST 域的配置信息	**check region-configuration**
手动激活 MST 域的配置	**active region-configuration**
退出 MST 域视图	**quit**

1.2.2 指定交换机为根交换机或备份根交换机

MSTP 可以通过计算来确定生成树的根交换机。用户也可以通过交换机提供的命令来指定当前交换机为根交换机。

可以通过下面的命令指定交换机为特定生成树的根交换机或备份根交换机。

请在系统视图下进行下列配置。

表1-4 指定交换机为生成树的树根或备份树根

操作	命令
指定交换机为特定生成树的根交换机	**stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-senconds*]
指定交换机为特定生成树的备份根交换机	**stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-senconds*]
取消当前交换机的根交换机或备份根交换机资格	**undo stp** [**instance** *instance-id*] **root**

设置当前交换机为根交换机或者备份根交换机之后，用户不能再修改交换机的优先级。

用户可以将当前交换机指定为生成树实例（由参数 **instance** *instance-id* 确定）的根交换机或备份根交换机。如果 *instance-id* 取值为 0，当前交换机将被指定为 CIST 的根交换机或备份根交换机。

当前交换机在各棵生成树实例中的根类型互相独立，它可以作为一棵生成树实例的根交换机或备份根交换机，同时也可以作为其他生成树实例的根交换机或备份根交换机；在同一棵生成树实例中，同一台交换机不能既作为根交换机，又作为备份根交换机。

当根交换机出现故障或被关机时，备份根交换机可以取代根交换机成为指定生成树实例的根交换机；但是此时如果用户设置了新的根交换机，则备份根交换机将不会成为根交换机。如果用户为一棵生成树实例配置了多个备份根交换机，当根交换机失效时，MSTP 将选择 MAC 地址最小的那个备份根交换机作为根交换机。

在设置根交换机和备份交换机时，用户可以同时指定交换网络的网络直径和 hello time 参数。关于网络直径和 hello time 的描述，可以参见配置任务“配置交换网络的网络直径”和“配置交换机的 Hello Time 时间参数”。

📖 **说明：**

当前交换机可以被指定为多棵生成树实例的树根，但是用户不能同时为一棵生成树实例指定两个或两个以上的根交换机，即不要在两台或两台以上的交换机上使用命令给同一棵生成树实例指定树根。

用户可以给同一棵生成树指定多个备份树根，即可以在两台或两台以上的交换机上使用命令给同一棵生成树实例指定备份树根。

一般情况下，建议用户给一棵生成树指定一个树根和多个备份树根。

缺省情况下，交换机既不作为生成树的根交换机，也不作为生成树的备份根交换机。

1.2.3 配置 MSTP 的工作模式

MSTP 和 RSTP 能够互相识别对方的协议报文，可以互相兼容。而 STP 无法识别 MSTP 的报文，MSTP 为了实现和 STP 的兼容，设定了两种工作模式：STP 兼容模式，MSTP 模式。在 STP 兼容模式下，交换机各个端口将发送 STP 报文；在 MSTP 模式下，交换机的各个端口将发送 MSTP 报文或者 STP 报文（如果端口上连接了 STP 交换机），并且具备多生成树的功能。

可以通过下面的命令配置 MSTP 的工作模式。MSTP 可以和 STP 协议互通，如果交换网络中存在运行 STP 协议的交换机，可以通过该命令配置当前的 MSTP 运行在 STP 兼容模式下，否则可以配置 MSTP 运行在 MSTP 模式下。

请在系统视图下进行下列配置。

表1-5 配置 MSTP 的运行模式

操作	命令
配置 MSTP 的运行模式为 STP 兼容模式	**stp mode stp**
配置 MSTP 的运行模式为 MSTP 模式	**stp mode mstp**
将 MSTP 的运行模式恢复为缺省值	**undo stp mode**

一般情况下，如果交换网络中存在运行 STP 的交换机，与 STP 交换机相连的端口自动从 MSTP 模式迁移到 STP 兼容模式下运行。但是如果运行 STP 的交换机被拆除后，此端口不能自动从 STP 兼容模式迁移到 MSTP 模式下运行。

缺省情况下，MSTP 运行在 MSTP 模式下。

1.2.4 配置交换机的 Bridge 优先级

交换机的 Bridge 优先级的大小决定了这台交换机是否能够被选作生成树的根。通过配置较小的 Bridge 优先级，可以达到指定某台交换机成为生成树树根的目的。支持 MSTP 的交换机在不同的生成树实例中可以拥有不同的优先级。

可以通过下面的命令配置指定交换机的在不同生成树实例中的 Bridge 优先级。

请在系统视图下进行下列配置。

表1-6 配置指定交换机的 Bridge 优先级

操作	命令
配置指定交换机的 Bridge 优先级	**stp** [**instance** *instance-id*] **priority** *priority*
将指定交换机的 Bridge 优先级恢复为缺省值	**undo stp** [**instance** *instance-id*] **priority**

配置交换机的优先级时，如果参数 **instance** *instance-id* 取值为 0，配置的优先级是交换机在 CIST 中的优先级。

⚠ 注意：

在生成树树根的选择过程中，如果交换机的 Bridge 优先级取值相同，则 MAC 地址最小的那台交换机将被选择为根。

缺省情况下，交换机的 Bridge 优先级取值为 32768。

1.2.5 配置 MST 域的最大跳数

MST 域的最大跳数限制了 MST 域的规模。配置在域根上的最大跳数将作为 MST 域的最大跳数。从域内的生成树的根交换机开始，域内的配置消息（即 BPDU）每经过一台交换机的转发，跳数就被减 1；交换机将丢弃收到的跳数为 0 的配置消息，使处于最大跳数外的交换机由于无法参与生成树的计算，从而限制了 MST 域的规模。

可以通过下面的命令配置 MST 域的最大跳数。

请在系统视图下进行下列配置。

表1-7 配置 MST 域的最大跳数

操作	命令
配置 MST 域的最大跳数	**stp max-hops** *hop*
将 MST 域的最大跳数恢复为缺省值	**undo stp max-hops**

MST 域的最大跳数越大，说明 MST 域的规模越大。只有配置在作为域根的交换机上的 MST 域的最大跳数才能限制 MST 域的规模。MST 域内的其他交换机将采用域根上的配置，即使本交换机也做了相应的配置。

缺省情况下，MST 域的最大跳数为 20。

1.2.6 配置交换网络的网络直径

交换网络中任意两台主机都通过特定路径彼此相连，这些路径由一系列交换机构成。网络直径指的是这些路径中交换机个数最多的那条路径，用路径经过的交换机个数来表征。

可以通过下面的命令配置交换网络的网络直径。

请在系统视图下进行下列配置。

表1-8 配置交换网络的网络直径

操作	命令
配置交换网络的网络直径	**stp bridge-diameter** *bridgenum*
将交换网络的网络直径恢复为缺省值	**undo stp bridge-diameter**

网络直径是表征网络规模的一个参数，网络直径越大，说明一个网络的规模越大。

当用户配置交换机的网络直径参数时，MSTP 通过计算自动将交换机的 hello time、forward-delay 以及 maximum-age 三个时间参数设置为一个较优的值。

设置网络直径只对 CIST 有效，对 MSTI（多生成树实例）无效。

缺省情况下，网络直径为 7，此时对应的三个时间也分别为它们的缺省值。

1.2.7 配置交换机的时间参数

交换机有三个时间参数：Forward Delay、Hello Time 和 Max Age。

Forward Delay 时间为交换机状态迁移机制。链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新配置消息无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话，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，根端口和指定端口重新开始数据转发之前要经历一个中间状态，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。

Hello Time 用于交换机检测链路是否存在故障。交换机每隔 Hello Time 时间会向周围的交换机发送 hello 报文，以确认链路是否存在故障。

Max Age 时间是用来判断配置消息是否“过时”的参数，交换机会将过时的配置消息丢弃。

可以通过下面的命令配置交换机的时间参数。

请在系统视图下进行下列配置。

表1-9 配置交换机的时间参数

操作	命令
配置指定交换机的 Forward Delay 时间参数	**stp timer forward-delay** *centiseconds*
将指定交换机的 Forward Delay 时间参数恢复为缺省值	**undo stp timer forward-delay**
配置交换机的 Hello Time 时间参数	**stp timer hello** *centiseconds*
将交换机的 Hello Time 时间参数恢复为缺省值	**undo stp timer hello**
配置交换机的 Max Age 时间参数	**stp timer max-age** *centiseconds*
将交换机的 Max Age 时间参数恢复为缺省值	**undo timer stp max-age**

整个交换网络中所有的交换机采用 CIST 的根交换机上的三个时间参数。

⚠ 注意：

交换机的 Forward Delay 时间参数的长短与交换网络的网络直径有关。一般来说，网络直径越大，Forward Delay 时间就应该配置地越长。需要注意的是，如果 Forward Delay 时间配置的过小，可能会引入临时的冗余路径；如果 Forward Delay 时间配置的过大，网络可能会较长时间不能恢复连通。建议用户采用缺省值。

合适的 Hello Time 时间值可以保证交换机能够及时发现网络中的链路故障，又不会占用过多的网络资源。建议用户使用缺省值。如果用户设置的 Hello Time 时间值过长，在链路发生丢包时，交换机会误以为链路出现了故障，从而引发网络设备重新计算生成树；如果用户设置的 Hello Time 时间值过短，交换机将频繁发送重复的配置消息，增加了交换机的负担，浪费了网络资源。

如果用户配置的 Max Age 时间过小，网络设备会频繁地计算生成树，而且有可能将网络拥塞误认成链路故障；如果用户配置的 Max Age 时间过大，网络设备很可能不能及时发现链路故障，不能及时重新计算生成树，从而降低网络的自适应能力。建议用户采用缺省值。

根交换机的 Hello Time、Forward Delay 以及 Maximum Age 三个时间参数取值之间应该满足如下公式，否则网络会频繁震荡：

2 × (forward-delay －1 second) >= maximum-age

maximum-age >= 2 × (hello time+ 1 second)

建议用户使用 **stp root primary** 命令指定交换网络的网络直径及 Hello Time，MSTP 会自动计算出这三个时间参数的比较优的取值。

缺省情况下，Forward Delay 时间为 1500 厘秒（即 15 秒），Hello Time 时间为 200 厘秒（即 2 秒），Max Age 时间为 2000 厘秒（即 20 秒）。

1.2.8 配置端口的最大发送速率

端口的最大发送速率是用来表示端口在每 Hello Time 时间内最多可发送多少个 MSTP 报文的参数。

以太网端口的最大发送速率与端口的物理状态和网络结构有关，用户可以根据实际的网络情况对其进行配置。

可以通过下面两种途径配置端口的最大发送速率。

1. 在系统视图下进行配置

请在系统视图下进行下列配置。

表1-10 配置端口的最大发送速率

操作	命令
配置端口的最大发送速率	**stp interface** *interface-list* **transit-limit** *packetnum*
将端口的最大发送速率恢复为缺省值	**undo stp interface** *interface-list* **transit-limit**

2. 在以太网端口视图下进行配置

请在以太网端口视图下进行下列配置。

表1-11 配置端口的最大发送速率

操作	命令
配置端口的最大发送速率	**stp transit-limit** *packetnum*
将端口的最大发送速率恢复为缺省值	**undo stp transit-limit**

以上两种方法都可以配置端口的最大发送速率。

此参数是一个相对值，没有单位。如果该参数被配置的过大，则每个 Hello Time 内发送的 MSTP 报文数就很多，从而占用过多的网络资源。建议用户采用缺省值。

缺省情况下，交换机上所有以太网端口的最大发送速率为 3。

1.2.9 配置端口为边缘端口或者非边缘端口

边缘端口是指：不直接与任何交换机连接，也不通过端口所连接的网络间接与任何交换机相连的端口。

可以通过下面两种途径来配置端口为边缘端口或者非边缘端口。

1. 在系统视图下进行配置

请在系统视图下进行下列配置。

表1-12 配置端口是否可以作为边缘端口

操作	命令
配置端口为边缘端口	**stp interface** *interface-list* **edged-port enable**
配置端口为非边缘端口	**stp interface** *interface-list* **edged-port disable**
将端口恢复为缺省的非边缘端口	**undo stp edged-port** *interface-list* **edged-port**

2. 在以太网端口视图下进行配置

请在以太网端口视图下进行下列配置。

表1-13 配置端口是否可以作为边缘端口

操作	命令
配置端口为边缘端口	**stp edged-port enable**
配置端口为非边缘端口	**stp edged-port disable**
将端口恢复为缺省的非边缘端口	**undo stp edged-port**

以上两种方法都可以配置端口为边缘端口或者非边缘端口。

用户如果将某个端口指定为边缘端口，那么当该端口由堵塞状态向转发状态迁移时，这个端口可以实现快速迁移，而无需等待延迟时间。用户只能将与终端链接的端口设置为边缘端口。在交换机没有使能 BPDU 保护的情况下，如果被设置为边缘端口的端口上收到来自其它端口的 BPDU 报文，则该端口会重新变为非边缘端口。如果交换机使能了 BPDU 保护，则该端口会被关闭。该参数对所有生成树实例有效，也就是说，当端口被配置为边缘端口或非边缘端口时，该端口在所有生成树实例上都被设置为边缘端口或非边缘端口。

在交换机没有使能 BPDU 保护的情况下，当端口收到 BPDU 后，即使用户设置为边缘端口，实际运行值也会变为非边缘端口。

缺省情况下，交换机所有以太网端口均被配置为非边缘端口。

📖 **说明：**

对于直接与终端相连的端口，请将该端口设置为边缘端口，同时启动 BPDU 保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。

1.2.10 配置端口的 Path Cost

Path Cost 即路径开销，是与端口相连的链路速率相关的参数。在支持 MSTP 的交换机上，端口在不同的生成树实例中可以拥有不同的路径开销。设置合适的路径开销可以使不同 VLAN 的流量沿不同的物理链路转发，从而实现按 VLAN 负荷分担的功能。

可以通过下面两种途径来配置端口的路径开销。

1. 在系统视图下进行配置

请在系统视图下进行下列配置。

表1-14 配置端口的路径开销

操作	命令
配置端口的路径开销	**stp interface** *interface-list* [**instance** *instance-id*] **cost** *cost*
将端口的路径开销恢复为缺省值	**undo stp interface** *interface-list* [**instance** *instance-id*] **cost**

2. 在以太网端口视图进行配置

请在以太网端口视图下进行下列配置。

表1-15 配置端口的路径开销

操作	命令
配置端口的路径开销	**stp** [**instance** *instance-id*] **cost** *cost*
将端口的路径开销恢复为缺省值	**undo stp** [**instance** *instance-id*] **cost**

以上两种方法都可以配置端口的路径开销。

端口路径开销改变时，MSTP 会重新计算端口的角色并进行状态迁移。*instance-id* 为 0 时表示设置为 CIST 的路径开销。

缺省情况下，由 MSTP 计算各个端口的路径开销。

1.2.11 配置端口的优先级

在生成树计算过程中端口优先级是确定该端口是否会被选为根端口的重要依据，同等条件下优先级高的端口将被选为根端口。在支持 MSTP 的交换机上，端口可以在不同的生成树实例中拥有不同的优先级，使同一端口在不同的生

成树实例中担任不同的角色，从而使不同 VLAN 的数据沿不同的物理路径传播，实现按 VLAN 进行负荷分担的功能。

可以通过下面两种途径来配置端口的优先级。

1. 在系统视图下进行配置

请在系统视图下进行下列配置。

表1-16 配置端口的优先级

操作	命令
配置端口的优先级	**stp interface** *interface-list* [**instance** *instance-id*] **port priority** *priority*
将端口的优先级恢复为缺省值	**undo stp interface** *interface-list* [**instance** *instance-id*] **port priority**

2. 在以太网端口视图下进行配置

请在以太网端口视图下进行下列配置。

表1-17 配置端口的优先级

操作	命令
配置端口的优先级	**stp** [**instance** *instance-id*] **port priority** *priority*
将端口的优先级恢复为缺省值	**undo stp** [**instance** *instance-id*] **port priority**

以上两种方法都可以配置端口的优先级。

端口优先级的改变时，MSTP 会重新计算端口的角色并进行状态迁移。一般情况下，配置的值越小，端口的优先级就越高。如果交换机所有的以太网端口采用相同的优先级参数值，则以太网端口的优先级高低就取决于该以太网端口的索引号。改变以太网端口的优先级会引起生成树重新计算。用户可以根据组网的实际需要来设置端口的优先级。

缺省情况下，交换机所有以太网端口的优先级为 128。

1.2.12 配置端口是否与点对点链路相连

点到点链路是两台交换机之间直接连接的链路。

可以通过下面两种途径来配置端口相连的链路是否是点到点链路。

1. 在系统视图下进行配置

请在系统视图下进行下列配置。

表1-18 配置端口是否与点对点链路相连

操作	命令
配置端口与点对点链路相连	**stp interface** *interface-list* **point-to-point force-true**
配置端口没有与点对点链路相连	**stp interface** *interface-list* **point-to-point force-false**
配置 MSTP 自动检测端口是否与点对点链路相连	**stp interface** *interface-list* **point-to-point auto**
将端口设置为缺省的自动检测是否与点对点链路相连的状态	**undo stp interface** *interface-list* **point-to-point**

2. 在以太网端口视图下进行配置

请在以太网端口视图下进行下列配置。

表1-19 配置端口是否与点对点链路相连

操作	命令
配置端口与点对点链路相连	**stp point-to-point force-true**
配置端口没有与点对点链路相连	**stp point-to-point force-false**
配置 MSTP 自动检测端口是否与点对点链路相连	**stp point-to-point auto**
将端口设置为缺省的自动检测是否与点对点链路相连的状态	**undo stp point-to-point**

以上两种方法都可以配置与端口相连的链路是否是点到点链路。

以点对点链路相连的两个端口，如果端口角色满足一定条件，则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。如果该参数被配置为自动模式，MSTP 可以自动检测当前的以太网端口是否与点对点链路相连。

📖 **说明：**

对于汇聚端口，只有汇聚端口的主端口才可以被配置成与点对点链路相连；一个端口工作在自协商模式，协商出来的工作模式是全双工，可以将此端口配置为点到点链路。

本配置对 CIST 和所有的 MSTI 有效，当端口被设置为与点对点链路相连或与非点对点链路相连，则该端口在所有生成树实例上均被设置为与点对点链路相连或与非点对点链路相连。如果端口实际物理链路不是点对点链路，用户错误配置为强制点对点链路，则有可能会引入临时回路。

缺省情况下，该参数被配置为 **auto**。

1.2.13 在端口上执行 mCheck 操作

在支持 MSTP 的交换机上端口有两种工作模式：STP 兼容模式、MSTP 模式。

假设在一个交换网络中，运行 MSTP 的交换机的端口连接着运行 STP 的交换机，该端口会自动迁移到 STP 兼容模式下工作；但是此时如果运行 STP 协议的交换机被拆离，该端口不能自动迁移到 MSTP 模式下运行，仍然会工作在 STP 兼容模式下。此时可以通过执行 mCheck 操作迫使其迁移到 MSTP 模式下运行。

可以通过下面两种途径在端口上执行 mCheck 操作。

1. 在系统视图下进行配置

请在系统视图下进行下列配置。

表1-20 在端口上执行 mCheck 操作

操作	命令
在端口上执行 mCheck 操作	**stp interface** *interface-list* **mcheck**

2. 在以太网端口视图下进行配置

请在以太网端口视图下进行下列配置。

表1-21 在端口上执行 mCheck 操作

操作	命令
在端口上执行 mCheck 操作	**stp mcheck**

以上两种方法都可以配置端口的 mCheck 变量。

需要注意的是，该命令必须在交换机运行 MSTP 的情况下进行配置，如果交换机的协议运行模式被配置为 STP 兼容模式，该命令无效。

1.2.14 配置交换机的保护功能

支持 MSTP 的交换机提供 BPDU 保护功能、Root 保护功能和环路保护功能。

对于接入层设备，接入端口一般直接与用户终端（如 PC 机）或文件服务器相连，此时接入端口被设置为边缘端口以实现这些端口的快速迁移；当这些端口接收到配置消息（BPDU 报文）时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑的震荡。这些端口正常情况下应该不会收到生成树协议的配置消息。如果有人伪造配置消息恶意攻击交换机，就会引起网络震荡。BPDU 保护功能可以防止这种网络攻击。

生成树的根交换机及备份交换机应该处于同一个域内，特别是对于 CIST 的根交换机和备份交换机，由于网络设计时一般会把 CIST 的根交换机和备份交换机放在一个高带宽的核心域内。但是由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根交换机有可能会收到优先级更高的配置消息，这样当前根交换机会失去根交换机的地位，引起网络拓扑结构的错误变动。这种不合法的变动，会导致原来应该通过高速链路的流量被牵引到低速链路上，导致网络拥塞。Root 保护功能可以防止这种情况的发生。

依靠不断接收上游交换机发送的 BPDU，交换机可以维持根端口和其他阻塞端口的状态。但是由于链路拥塞或者单向链路故障，这些端口会收不到上游交换机的 BPDU。此时交换机会重新选择根端口，根端口会转变为指定端口，而阻塞端口会迁移到转发状态，从而交换网络中会产生环路。环路保护功能会抑制这种环路的产生。在启动了环路保护功能后，根端口的角色不会迁移，阻塞端口会一直保持在 Discarding 状态，不转发报文，从而不会在网络中形成环路。

可以通过下面的命令来配置交换机的保护功能。

请在相应视图下进行下列配置。

表1-22 配置交换机的保护功能

操作	命令
配置交换机的 BPDU 保护功能（系统视图）	**stp bpdu-protection**
恢复配置交换机的 BPDU 保护功能为缺省的关闭状态（系统视图）	**undo stp bpdu-protection**
配置交换机的 Root 保护功能（系统视图）	**stp interface** *interface-list* **root-protection**
恢复配置交换机的 Root 保护功能为缺省的关闭状态（系统视图）	**undo stp interface** *interface-list* **root-protection**
配置交换机的 Root 保护功能（以太网端口视图）	**stp root-protection**
恢复配置交换机的 Root 保护功能为缺省的关闭状态（以太网端口视图）	**undo stp root-protection**
配置交换机的环路保护功能（以太网端口视图）	**stp loop-protection**
恢复配置交换机的环路保护功能为缺省的关闭状态（以太网端口视图）	**undo stp loop-protection**

交换机上启动了 BPDU 保护功能以后，如果边缘端口收到了配置消息，系统就将这些端口关闭，同时通知网管这些端口被 MSTP 关闭。被关闭的端口只能由网络管理人员恢复。

对于设置了 Root 保护功能的端口，其在所有实例上的端口角色只能保持为指定端口。一旦这种端口上收到了优先级高的配置消息，即其将被选择为非指定端口时，这些端口的状态将被设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在足够长的时间内没有收到更优的配置消息时，端口会恢复原来的正常状态。

在对一个端口进行配置的时候，在 Loop 保护功能，Root 保护功能或者边缘端口设置三个配置中，同一时刻只能有一个配置生效。

缺省情况下，交换机不启动 BPDU 保护功能、Root 保护功能和环路保护功能。

1.2.15 开启设备 MSTP 特性

可以通过下面的命令开启设备的 MSTP 特性。

请在系统视图下进行下列配置。

表1-23 开启/关闭设备 MSTP 特性

操作	命令
开启设备 MSTP 特性	**stp enable**
关闭设备 MSTP 特性	**stp disable**
将设备 MSTP 特性恢复为缺省的关闭状态	**undo stp**

只有开启了设备的 MSTP 特性，MSTP 的其他配置才能生效。

缺省情况下，不运行 MSTP。

1.2.16 开启/关闭端口 MSTP 特性

可以通过下面的命令开启/关闭端口的 MSTP 特性。为了灵活地控制 MSTP 工作，可以关闭交换机上特定以太网端口的 MSTP 特性，使这些端口不参与生成树计算，节省交换机的 CPU 资源。

可以通过下面两种途径来开启/关闭端口 MSTP 特性。

1. 在系统视图下进行配置

请在系统视图下进行下列配置。

表1-24 开启/关闭端口 MSTP 特性

操作	命令
在端口上开启 MSTP	**stp interface** *interface-list* **enable**
在端口上关闭 MSTP	**stp interface** *interface-list* **disable**

2. 在以太网端口视图下进行配置

请在以太网端口视图下进行下列配置。

表1-25 开启/关闭端口 MSTP 特性

操作	命令
在端口上开启 MSTP	**stp enable**
在端口上关闭 MSTP 协议	**stp disable**

以上两种方法都可以实现开启或关闭端口上的 MSTP 特性。

需要注意的是，关闭以太网端口上的 MSTP 后，可能会产生冗余路径。

缺省情况下，设备 MSTP 特性开启后所有端口上的 MSTP 特性都是开启的。

1.3 MSTP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后 MSTP 的运行情况。用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **reset** 命令可以将有关 MSTP 的统计信息清除。在用户视图下执行 **debugging** 命令可以对 MSTP 模块进行调试。

表1-26 MSTP 显示和调试

操作	命令
显示本设备及当前端口的配置信息	**display stp instance** *instance-id* [**interface** *interface-list*] [**brief**]
显示域的配置信息	**display stp region-configuration**
清除 MSTP 的统计信息	**reset stp** [**interface** *interface-list*]
打开/关闭 MSTP 对指定端口的调试开关（收发报文、事件、错误等）	[**undo**] **debugging stp** [**interface** *interface-list*] { **packet** | **event** }
打开/关闭 MSTP 的全局调试开关	[**undo**] **debugging stp** { **global-event** | **global-error** | **all** }
打开/关闭 MSTP 对指定实例的调试开关	[**undo**] **debugging stp instance** *instance-id*

目 录

第1章 802.1x 配置

1.1 802.1x 简介

1.1.1 802.1x 标准简介

IEEE 802.1x 标准（以下简称 802.1x）的主要内容是一种基于端口的网络接入控制（Port Based Network Access Control）协议，IEEE 于 2001 年颁布该标准文本并建议业界厂商使用其中的协议作为局域网用户接入认证的标准协议。802.1x 的提出起源于 IEEE 802.11 标准——无线局域网用户接入协议标准，其最初目的主要是解决无线局域网用户的接入认证问题；但由于它的原理对于所有符合 IEEE 802 标准的局域网具有普适性，因此后来它在有线局域网中也得到了广泛的应用。

在符合 IEEE 802 标准的局域网中，只要与局域网接入控制设备如 LANSwitch 相接，用户就可以与局域网连接并访问其中的设备和资源。但是对于诸如电信接入、商务局域网（典型的例子是写字楼中的 LAN）以及移动办公等应用场合，局域网服务的提供者普遍希望能对用户的接入进行控制，为此产生了本章开始就提到的对“基于端口的网络接入控制”的需求。

顾名思义，“基于端口的网络接入控制”是指在局域网接入控制设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源——相当于连接被物理断开。

802.1x 定义了基于端口的网络接入控制协议，并且仅定义了接入设备与接入端口间点到点这一种连接方式。其中端口既可以是物理端口，也可以是逻辑端口。典型的应用环境如：以太网交换机的每个物理端口仅连接一个用户的计算机工作站（基于物理端口），IEEE 802.11 标准定义的无线 LAN 接入环境（基于逻辑端口）等。

1.1.2 802.1x 体系结构

使用 802.1x 的系统为典型的 C/S（Client/Server）体系结构，包括三个实体，如下图所示分别为：Supplicant System（接入系统）、Authenticator System（认证系统）以及 Authentication Server System（认证服务器系统）。

局域网接入控制设备需要提供 802.1x 的认证系统（Authenticator System）部分；用户侧的设备如计算机等需要安装 802.1x 的客户端（Supplicant）软件，如华为公司提供的 802.1x 客户端（或如 Windows XP 自带的 802.1x 客户端）；802.1x 的认证服务器系统（Authentication Server System）则一般驻留在运营商的 AAA 中心。

Authenticator 与 Authentication Server 间通过 EAP（Extensible Authentication Protocol，可扩展认证协议）帧交换信息，Supplicant 与 Authenticator 间则以 IEEE 802.1x 所定义的 EAPoL（EAP over LANs，局域网上的 EAP）帧交换信息，EAP 帧中封装了认证数据，该认证数据将被封装在其它 AAA 上层协议（如 RADIUS）的报文中以穿越复杂的网络到达 Authentication Server，这一过程被称为 EAP Relay。

Authenticator 的端口又分为两种：非受控端口（Uncontrolled Port）和受控端口（Controlled Port）。非受控端口始终处于双向连通状态，用户接入设备可以随时通过这些端口访问网络资源以获得服务；受控端口只有在用户接入设备通过认证后才处于连通状态，才允许用户通过其进一步访问网络资源。

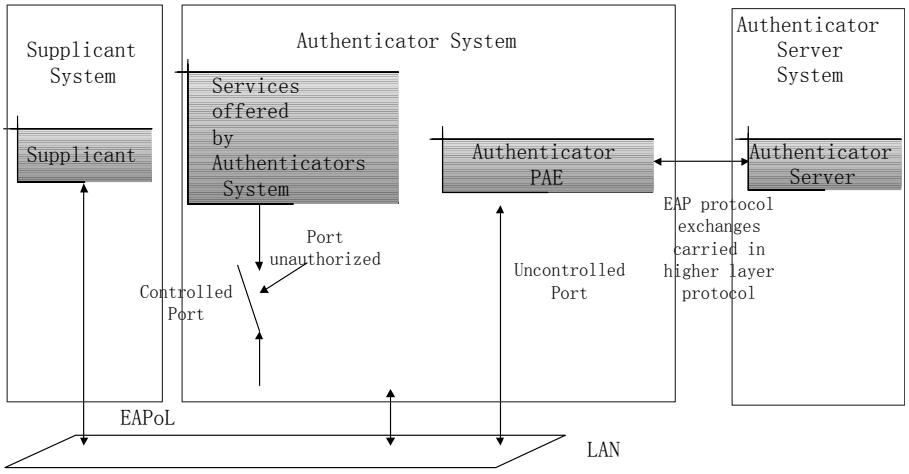


图1-1 802.1x 体系结构

1.1.3 802.1x 的认证过程

802.1x 通过 EAP 帧承载认证信息。标准中共定义了如下几种类型的 EAP 帧：

- EAP-Packet：认证信息帧，用于承载认证信息。
- EAPoL-Start：认证发起帧，Supplicant 主动发起的认证发起帧。
- EAPoL-Logoff：退出请求帧，主动终止已认证状态。
- EAPoL-Key：密钥信息帧，支持对 EAP 报文的加密。

- EAPoL-Encapsulated-ASF-Alert：用于支持 Alert Standard Forum（ASF）的 Alerting 消息。

其中 EAPoL-Start、EAPoL-Logoff 和 EAPoL-Key 仅在 Supplicant 和 Authenticator 间存在；EAP-Packet 信息由 Authenticator System 重新封装后传递到 Authentication Server System；EAPoL-Encapsulated-ASF-Alert 与网管信息相关，由 Authenticator 终结。

由上述的原理我们可以看到，802.1x 提供了一个用户身份认证的实现方案，但是仅仅依靠 802.1x 是不足以实现该方案的——接入设备的管理者还要对 AAA 方法进行配置，选择使用 RADIUS 或本地认证方法，以配合 802.1x 完成用户的身份认证。AAA 方法的具体配置细节，请参见本书的“AAA 和 RADIUS 协议配置”章节。

1.1.4 802.1x 在以太网交换机中的实现

Quidway S5000 系列以太网交换机在 802.1x 的实现中，不仅支持协议所规定的端口接入认证方式，还对其进行了扩展、优化：

- 支持一个物理端口下挂接多个用户的应用场合；
- 接入控制方式（即对用户的认证方式）不仅可以基于端口，还可以基于 MAC 地址。

这样可极大地提高系统的安全性和可管理性。

1.2 802.1x 配置

802.1x 本身的各项配置任务都可以在以太网交换机的系统视图下完成。当全局 802.1x 没有开启时，可以对端口的 802.1x 状态进行配置，其配置项会在开启全局 802.1x 后生效。

📖 **说明：**

(1) 请不要同时启动 802.1x 与 RSTP（或 MSTP），两者同时启动时不能保证交换机的正常工作。
(2) 如果端口启动了 802.1x，则不能配置该端口的最大 MAC 地址学习个数（通过命令 **mac-address max-mac-count** 配置），反之，如果端口配置了最大 MAC 地址学习个数，则禁止在该端口上启动 802.1x。

802.1x 的配置包括：

- 开启/关闭 802.1x 特性
- 设置端口接入控制的模式

- 设置端口接入控制方式
- 检测通过代理登录交换机的用户
- 设置端口接入用户数量的最大值
- 配置 802.1x 用户的认证方法
- 设置允许 DHCP 触发认证
- 设置认证请求帧的可重复发送次数
- 设置 802.1x 的握手报文的发送时间间隔
- 设置定时器参数
- 打开/关闭 quiet period 定时器

在以上的配置任务中，第一项任务是必配的，否则 802.1x 无法发挥作用；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

1.2.1 开启/关闭 802.1x 特性

可以通过下面的命令开启/关闭指定端口上的 802.1x 特性；当不指定任何确定的端口时，开启/关闭全局的 802.1x 特性。

请在系统视图或以太网端口视图下进行下列配置。

表1-1 开启/关闭 802.1x 特性

操作	命令
开启 802.1x 特性	**dot1x** [**interface** *interface-list*]
关闭 802.1x 特性	**undo dot1x** [**interface** *interface-list*]

各端口的 802.1x 状态在全局 802.1x 没有开启之前可以配置，但不起作用；在全局 802.1x 启动后，各端口配置会立即生效。

缺省情况下，全局及端口的 802.1x 特性均为关闭状态。

1.2.2 设置端口接入控制的模式

可以通过下面的命令来设置 802.1x 在指定端口上进行接入控制的模式。当没有指定任何确定的端口时，设置的是所有端口进行接入控制的模式。

请在系统或以太网端口视图下进行下列配置。

表1-2 设置端口接入控制的模式

操作	命令
设置端口接入控制的模式	**dot1x port-control** {**authorized-force** | **unauthorized-force** | **auto** } [**interface** *interface-list*]
将端口接入控制的模式恢复为缺省值	**undo dot1x port-control** [**interface** *interface-list*]

缺省情况下，802.1x 在端口上进行接入控制的模式为 **auto**（自动识别模式，又称为协议控制模式），即：端口初始状态为非授权状态，仅允许 EAPoL 报文收发，不允许用户访问网络资源；如果认证流程通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常见的情况。

1.2.3 设置端口接入控制方式

可以通过下面的命令来设置 802.1x 在指定端口上进行接入控制方式。当没有指定任何确定的端口时，设置的是所有端口进行接入控制的方式。

请在系统或以太网端口视图下进行下列配置。

表1-3 设置端口接入控制方式

操作	命令
设置端口接入控制方式	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]
将端口接入控制方式恢复为缺省值	**undo dot1x port-method** [**interface** *interface-list*]

缺省情况下，802.1x 在端口上进行接入控制方式为 **macbased**，即基于 MAC 地址进行认证。

1.2.4 检测通过代理登录交换机的用户

可以通过下面的命令实现交换机对通过代理登录的用户的检测及相关控制。

请在系统或以太网端口视图下进行下列配置。

表1-4 设置通过代理登录交换机的用户的检测及控制

操作	命令
使能对通过代理登录交换机的用户的检测及控制	**dot1x supp-proxy-check** { **logoff	trap** } [**interface** *interface-list*]
取消对通过代理登录交换机的用户的检测及控制	**undo dot1x supp-proxy-check** { **logoff	trap** } [**interface** *interface-list*]

1.2.5 设置端口接入用户数量的最大值

可以通过下面的命令来设置 802.1x 在指定端口上可容纳接入用户数量的最大值。当没有指定任何确定的端口时，指示所有端口都可容纳相同数量的接入用户。

请在系统或以太网端口视图下进行下列配置。

表1-5 设置端口接入用户数量的最大值

操作	命令
设置端口接入用户数量的最大值	**dot1x max-user** *user-number* [**interface** *interface-list*]
将端口接入用户数量的最大值恢复为缺省值	**undo dot1x max-user** [**interface** *interface-list*]

缺省情况下，802.1x 在 S5000 系列以太网交换机所有的端口上都允许最多有 256 个接入用户。

1.2.6 设置允许 DHCP 触发认证

可以通过下面的命令来设置 802.1x 是否允许以太网交换机在用户运行 DHCP、申请动态 IP 地址时就触发对其的身份认证。

请在系统视图下进行下列配置。

表1-6 设置允许 DHCP 触发认证

操作	命令
允许 DHCP 触发认证	**dot1x dhcp-launch**
不允许 DHCP 触发认证	**undo dot1x dhcp-launch**

缺省情况下，不允许在用户运行 DHCP 申请动态 IP 地址时就触发对其的身份认证。

1.2.7 设置 802.1x 用户的认证方法

可以通过下面的命令来设置 802.1x 用户的认证方法。目前提供 3 种认证方法：PAP 认证（该功能的实现，需要 RADIUS 服务器支持 PAP 认证）、CHAP 认证（该功能的实现，需要 RADIUS 服务器支持 CHAP 认证）、EAP 中继认证（直接把认证信息以 EAP 报文的形式发送给 RADIUS 服务器，该功能的实现，需要 RADIUS 服务器支持 EAP 认证）

请在系统视图下进行下列配置。

表1-7 设置 802.1x 用户认证方法

操作	命令
设置 802.1x 用户的认证方法	**dot1x authentication-method** { **chap** | **pap** | **eap md5-challenge** }
恢复缺省 802.1x 用户认证方法	**undo dot1x authentication-method**

缺省情况下，交换机 802.1x 用户认证方法为 CHAP 认证。

1.2.8 设置认证请求帧的最大可重复发送次数

可以通过下面的命令来设置以太网交换机可重复向接入用户发送认证请求帧的最大次数。

请在系统视图下进行下列配置。

表1-8 设置认证请求帧的最大可重复发送次数

操作	命令
设置认证请求帧的最大可重复发送次数	**dot1x retry** *max-retry-value*
将认证请求帧的最大可重复发送次数恢复为缺省值	**undo dot1x retry**

缺省情况下，*max-retry-value* 为 3，即交换机最多可重复向接入用户发送 3 次认证请求帧。

1.2.9 设置 802.1x 的握手报文的发送时间间隔

可以通过下面的命令来设置 802.1x 的握手报文的发送时间间隔。配置后，系统以此间隔为周期发送握手请求报文。如果 **dot1x retry** 命令配置重试次数为 N，则系统连续 N 次没有收到客户端的响应报文，就认为用户已经下线，将用户置为下线状态。

请在系统视图下进行下列配置。

表1-9 设置 802.1x 的握手报文的发送时间间隔

操作	命令
设置 802.1x 的握手报文的发送时间间隔	**dot1x timer handshake-period** *interval*
恢复时间间隔为缺省值	**undo dot1x timer handshake-period**

缺省情况下，握手报文的发送时间间隔为 15 秒。

1.2.10 配置定时器参数

可以通过下面的命令来配置 802.1x 的各项定时器参数。

请在系统视图下进行下列配置。

表1-10 配置定时器参数

操作	命令
配置定时器参数	**dot1x timer** { **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **supp-timeout** *supp-timeout-value* | **server-timeout** *server-timeout-value* }
将定时器参数恢复为缺省值	**undo dot1x timer** { **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout** }

其中：

quiet-period：静默定时器。当对 802.1x 用户认证失败以后，Authenticator 设备需要静默一段时间（该时间由静默定时器设置）后再重新发起认证，在静默期间，Authenticator 设备不进行 802.1x 认证的相关处理。

quiet-period-value：静默定时器设置的时长，取值范围 10～120，单位为秒。

server-timeout：Authentication Server 超时定时器。若在该定时器设置的时长内，Authentication Server 未成功响应，Supplicant 设备将重发认证请求报文。

server-timeout-value：Authentication Server 超时定时器设置的时长，取值范围为 100～300，单位为秒。

supp-timeout：Supplicant 认证超时定时器。若在该定时器设置的时长内，Supplicant 设备未成功响应，Authenticator 设备将重发认证请求报文。

supp-timeout-value：Supplicant 认证超时定时器设置的时长，取值范围为 10～120，单位为秒。

tx-period：传送超时定时器。若在该定时器设置的时长内，Supplicant 设备未成功发送认证应答报文，则 Authenticator 设备将重发认证请求报文。

tx-period-value：传送超时定时器设置的时长，取值范围为 10～120，单位为秒。

缺省情况下，*quiet-period-value* 为 60 秒；*tx-period-value* 为 30 秒；*supp-timeout-value* 为 30 秒；*server-timeout-value* 为 100 秒。

1.2.11 打开/关闭 quiet-period 定时器

可以通过下面的命令来打开/关闭 Authenticator 设备（如 Quidway 系列以太网交换机）的 quiet-period 定时器。当 802.1x 用户认证失败以后，Authenticator 设备需要静默一段时间（该时间由静默定时器设置）后再重新发起认证，在静默期间，Authenticator 设备不进行 802.1x 认证的相关处理。

请在系统视图下进行下列配置。

表1-11 打开/关闭 quiet-period 定时器

操作	命令
打开 quiet-period 定时器	**dot1x quiet-period**
关闭 quiet-period 定时器	**undo dot1x quiet-period**

1.3 802.1x 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 802.1x 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可清除 802.1x 相关配置。

在用户视图下，执行 **debugging** 命令可对 802.1x 进行调试。

表1-12 802.1x 的显示和调试

操作	命令
清除 802.1x 的统计信息	**reset dot1x statistics** [**interface** *interface-list*]
显示 802.1x 的配置、运行情况和统计信息	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]
打开 802.1x 的错误/事件/报文/全部调试开关	**debugging dot1x** { **error** | **event** | **packet** | **all** }
关闭 802.1x 的错误/事件/报文/全部调试开关	**undo debugging dot1x** { **error** | **event** | **packet** | **all** }

1.4 802.1x 典型配置举例

1. 组网需求

如下图所示，某用户的工作站与以太网交换机的端口 GigabitEthernet 0/1 相连接。

交换机的管理者希望在各端口上对用户接入进行认证，以控制其访问 Internet；接入控制模式要求是基于 MAC 地址的接入控制。

所有 AAA 接入用户都属于一个缺省的域：huawei163.net，该域最多可容纳 30 个用户；认证时，先进行 RADIUS 认证，如果 RADIUS 服务器没有响应再转而进行本地认证；计费时，如果 RADIUS 计费失败则切断用户连接使其下线；此外，接入时在用户名后不添加域名，正常连接时如果用户有超过 20 分钟流量持续小于 2000Byte/s 的情况则切断其连接。

由两台 RADIUS 服务器组成的服务器组与交换机相连，其 IP 地址分别为 10.11.1.1 和 10.11.1.2，要求使用前者作为主认证/从计费服务器，使用后者作为从认证/主计费服务器；设置系统与认证 RADIUS 服务器交互报文时的加密密码为“name”、与计费 RADIUS 服务器交互报文时的加密密码“money”，设置系统在向 RADIUS 服务器发送报文后 5 秒种内如果没有得到响应就向其重新发送报文，重复发送报文的次数总共为 5 次，设置系统每 15 分钟就向 RADIUS 服务器发送一次实时计费报文，指示系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

本地 802.1x 接入用户的用户名为 localuser，密码为 localpass，使用明文输入，闲置切断功能处于打开状态。

2. 组网图

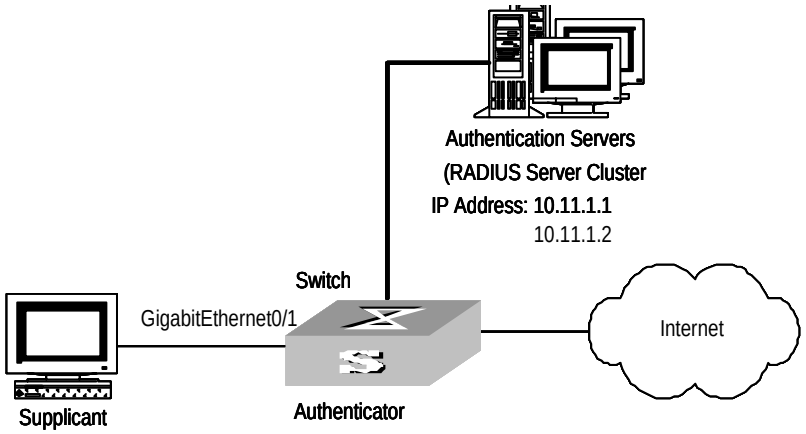


图1-2 启动 802.1x 和 RADIUS 对接入用户进行 AAA 操作

3. 配置步骤

说明：

下述各配置步骤包含了大部分 AAA/RADIUS 协议配置命令，对这些命令的介绍，请参见“AAA 和 RADIUS 协议配置”一章的相关章节。
此外，接入用户工作站和 RADIUS 服务器上的配置略。

开启指定端口 GigabitEthernet 0/1 的 802.1x 特性。

[Quidway] dot1x interface GigabitEthernet 0/1

设置接入控制方式（该命令可以不配置，因为端口的接入控制在缺省情况下就是基于 MAC 地址的）。

[Quidway] dot1x port-method macbased interface GigabitEthernet 0/1

创建 RADIUS 组 radius1 并进入其视图。

[Quidway] radius scheme radius1

设置主认证/计费 RADIUS 服务器的 IP 地址。

[Quidway-radius-radius1] primary authentication 10.11.1.1

[Quidway-radius-radius1] primary accounting 10.11.1.2

设置从认证/计费 RADIUS 服务器的 IP 地址。

[Quidway-radius-radius1] secondary authentication 10.11.1.2

[Quidway-radius-radius1] secondary accounting 10.11.1.1

设置系统与认证 RADIUS 服务器交互报文时的加密密码。

[Quidway -radius-radius1] key authentication name

设置系统与计费 RADIUS 服务器交互报文时的加密密码。

[Quidway-radius-radius1] key accounting money

设置系统向 RADIUS 服务器重发报文的时间间隔与次数。

[Quidway-radius-radius1] timer 5

[Quidway-radius-radius1] retry 5

设置系统向 RADIUS 服务器发送实时计费报文的时间间隔。

[Quidway-radius-radius1] timer realtime-accounting 15

指示系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

[Quidway-radius-radius1] user-name-format without-domain

[Quidway-radius-radius1] quit

创建用户域 huawei163.net 并进入其视图。

[Quidway] domain huawei163.net

指定 radius1 为该域用户的 RADIUS 服务器组。

[Quidway-isp-huawei163.net] radius-scheme radius1

设置该域最多可容纳 30 个用户。

[Quidway-isp-huawei163.net] access-limit enable 30

启动闲置切断功能并设置相关参数。

[Quidway-isp-huawei163.net] idle-cut enable 20 2000

添加本地接入用户。

[Quidway] local-user localuser

[Quidway-luser-localuser] service-type lan-access

[Quidway-luser-localuser] password simple localpass

开启全局 802.1x 特性。

[Quidway] dot1x

第2章 AAA 和 RADIUS 协议配置

2.1 AAA 和 RADIUS 协议简介

2.1.1 AAA 概述

AAA 是 Authentication，Authorization and Accounting（认证、授权和计费）的简称，它提供了一个用来对认证、授权和计费这三种安全功能进行配置的一致性框架，实际上是对网络安全的一种管理。

这里的网络安全主要是指访问控制，包括：

- 哪些用户可以访问网络服务器？
- 具有访问权的用户可以得到哪些服务？
- 如何对正在使用网络资源的用户进行计费？

针对以上问题，AAA 必须提供下列服务：

- 认证：验证用户是否可获得访问权。
- 授权：授权用户可使用哪些服务。
- 计费：记录用户使用网络资源的情况。

AAA 一般采用客户/服务器结构：客户端运行于被管理的资源侧，服务器上集中存放用户信息。因此，AAA 框架具有良好的可扩展性，并且容易实现用户信息的集中管理。

2.1.2 RADIUS 协议概述

如前所述，AAA 是一种管理框架，因此，它可以用多种协议来实现。在实践中，人们最常使用 RADIUS 协议来实现 AAA。

1. 什么是 RADIUS

RADIUS 是 Remote Authentication Dial-In User Service（远程认证拨号用户服务）的简称，它是一种分布式的、客户机/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常被应用在既要求较高安全性、又要求维持远程用户访问的各种网络环境中（例如，它常被应用来管理使用串口和调制解调器的大量分散拨号用户）。RADIUS 系统是 NAS（Network Access Server）系统的重要辅助部分。

当 RADIUS 系统启动后，如果用户想要通过与 NAS（PSTN 环境下的拨号接入服务器或以太网环境下带接入功能的以太网交换机）建立连接从而获得访问其它网络的权利或取得使用某些网络资源的权利时，NAS，也就是 RADIUS 客户端将把用户的认证、授权和计费请求传递给 RADIUS 服务器。RADIUS 服务器上有一个用户数据库，其中包含了所有的用户认证和网络服务访问信息。RADIUS 服务器将在接收到 NAS 传来的用户请求后，通过对用户数据库的查找、更新，完成相应的认证、授权和计费工作，并把用户所需的配置信息和计费统计数据返回给 NAS——在这里，NAS 起到了控制接入用户及对应连接的作用，而 RADIUS 协议则规定了 NAS 与 RADIUS 服务器之间如何传递用户配置信息和计费信息。

NAS 和 RADIUS 之间信息的交互是通过将信息承载在 UDP 报文中来完成的。在这个过程中，交互双方将使用密钥对报文进行加密，以保证用户的配置信息（如密码）被加密后才在网络上传递，从而避免它们被侦听、窃取。

2. RADIUS 操作

RADIUS 服务器对用户的认证过程通常需要利用接入服务器等设备的代理认证功能，通常整个操作步骤如下：首先，客户端向 RADIUS 服务器发送请求报文（该报文中包含用户名和加密口令）；然后，客户端会收到 RADIUS 服务器的响应报文，如 ACCEPT 报文、REJECT 报文等（其中，ACCEPT 报文表明用户通过认证；REJECT 报文表明用户没有通过认证，需要用户重新输入用户名和口令，否则访问被拒绝）。

2.1.3 AAA/RADIUS 在以太网交换机中的实现

由前面的概述，我们可以明白，在这样一个 AAA/RADIUS 框架中，Quidway 系列以太网交换机是作为用户接入设备即 NAS，相对于 RAIDUS 服务器来说，Quidway 系列以太网交换机是 RADIUS 系统的客户端；换句话说，AAA/RADIUS 在 Quidway 系列以太网交换机中实现的是其客户端部分。Quidway 系列以太网交换机参与的、使用 RADIUS 认证的组网示意图如下所示。

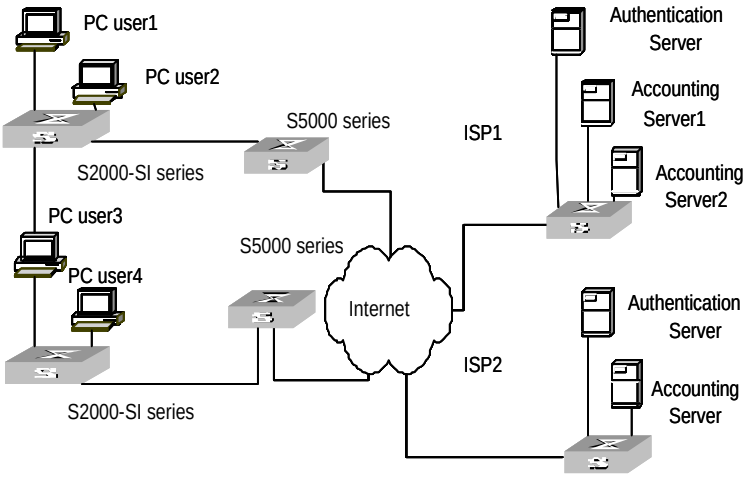


图2-1 S5000 系列使用 RADIUS 认证的典型组网图

2.2 AAA 配置

AAA 的配置包括：

- 创建/删除 ISP 域
- 配置 ISP 域的相关属性
- 创建本地用户
- 设置本地用户的属性
- 强制切断用户连接

在以上的配置任务中，创建 ISP 域是必需的，否则无法区分接入用户的属性；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.2.1 创建/删除 ISP 域

什么是 ISP（Internet Service Provider）域？简单点说，ISP 域即 ISP 用户群，一个 ISP 域即是由同属于一个 ISP 的用户构成的用户群。一般说来，在“userid@isp-name”形式（例如 gw20010608@huawei163.net）的用户名中，“@”后的“isp-name”（如例中的“huawei163.net”）即为 ISP 域的域名。在 Qudiway 系列以太网交换机对用户进行接入控制时，对于用户名为“userid@isp-name”形式的 ISP 用户，系统就将把“userid”作为用于身份认证的用户名，把“isp-name”作为域名。

引入 ISP 域的设置是为了支持多 ISP 的应用环境：在这种环境中，同一个接入设备接入的有可能是不同 ISP 的用户。由于各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能各不相同，因此有必要通过设

置 ISP 域的方法把它们区别开。在 Qudiway 系列以太网交换机的 ISP 域视图下，可以为每个 ISP 域配置包括 AAA 策略（使用的 RADIUS 服务器组等）在内的一整套单独的 ISP 域属性。

对于 Qudiway 系列以太网交换机来说，每个接入用户都属于一个 ISP 域。系统中最多可以配置 16 个 ISP 域。如果某个用户在登录时没有上报 ISP 域名，则系统将把它归于缺省的 ISP 域。

请在系统视图下进行下列配置。

表2-1 创建/删除 ISP 域

操作	命令
创建 ISP 域或进入指定 ISP 域视图	**domain** [*isp-name* | **default** { **disable** | **enable** *isp-name* }]
删除指定的 ISP 域	**undo domain** *isp-name*

缺省情况下，系统创建了一个名为“system”的 ISP 域，其各项属性均使用缺省值。

2.2.2 配置 ISP 域的相关属性

ISP 域的相关属性包括引用的 RADIUS 服务器组、ISP 域的状态、可容纳接入用户数的最大数值和用户闲置切断开关设置。其中：

- 引用的 RADIUS 服务器组指定的是该 ISP 域下所有用户所使用的 RADIUS 服务器组的组名。该 RADIUS 服务器组可被用于进行 RADIUS 认证和 RADIUS 计费。缺省情况下，使用缺省的 RADIUS 服务器组。此命令需与 RADIUS 服务器和服务器组的设置命令联合使用，具体请参见本章后面的 RADIUS 配置一节。
- 每个 ISP 域有两种状态：active 或 block。当指示某个 ISP 域处于 active 状态时，允许该域下的用户请求网络服务；当指示某个 ISP 域处于 block 状态时，不允许该域下的用户请求网络服务，但是不影响已经在线的用户。一个 ISP 域在刚被创建时是处于 active 状态的，即：在这个时候，允许任何属于该域的用户请求网络服务。
- 可容纳接入用户数的最大值用来指定该 ISP 域最多可容纳多少个接入用户。缺省情况下，对任何一个 ISP 域，没有任何可容纳接入用户数的限制。
- 用户闲置切断功能是当用户在设定的时间内流量小于设定的流量时，切断该用户的连接。

请在 ISP 域视图下进行下列配置。

表2-2 配置 ISP 域的相关属性

操作	命令
指定引用的 RADIUS 服务器组	**radius-scheme** *radius-scheme-name*
恢复域为默认的 RADIUS 组	**undo radius-scheme**
设置 ISP 域的状态	**state** { **active** | **block** }
指定可容纳接入用户数的最大值	**access-limit** { **disable** | **enable** *max-user-number* }
恢复可容纳接入用户数到缺省设置	**undo access-limit**
设置用户闲置切断	**idle-cut** { **disable** | **enable** *minute* flow}

缺省情况下，当一个 ISP 域被创建以后，其状态为 **active**；其可容纳的接入用户没有数量限制；不设置闲置切断。

2.2.3 创建本地用户

所谓本地用户，是指在 NAS 上设置的一组用户的集合。该集合以用户名为用户的唯一标识。为使某个请求网络服务的用户可以进行本地认证，需要在 NAS 上添加相应的本地用户。

请在系统视图下进行下列配置。

表2-3 创建/删除本地用户

操作	命令
添加本地用户	**local-user** *user-name*
删除所有本地户	**undo local-user all**
删除指定类型的本地用户	**undo local-user** { *user-name* | **all** [**service-type** { **lan-access** | **ftp** | **telnet** | **ssh** }] }

缺省情况下，系统中没有任何本地用户。

2.2.4 设置本地用户的属性

本地用户的属性包括：用户密码、用户状态、用户业务类型等的设置。

请在系统视图下进行下列设置。

表2-4 设置本地用户密码设置方式

操作	命令
设置本地用户密码设定方式	**local-user password-display-mode** { **cipher-force** | **auto** }
取消设置的本地用户密码设置方式	**undo local-user password-display-mode**

其中，**auto** 表示按照用户配置的密码显示方式（参考下面表格中 **password** 命令）显示，**cipher-force** 表示所有接入用户的密码显示必须采用密文方式。

请在本地用户视图下进行下列配置。

表2-5 设置/取消指定用户的相关属性

操作	命令
设置指定用户的密码	**password** { **simple** | **cipher** } *password*
取消指定用户的密码设置	**undo password**
设置指定用户的状态	**state** { **active** | **block** }
取消指定用户的状态	**undo state** { **active** | **block** }
设置指定用户的服务类型	**service-type** { **ftp** [**ftp-directory** *directory*] | **lan-access** | **ssh** [**level** *level* | **telnet** [**level** *level*]] | **telnet** [**level** *level* | **ssh** [**level** *level*]] }
取消指定用户的服务类型	**undo service-type** { **ftp** [**ftp-directory**] | **lan-access** | **ssh** [**level** | **telnet** [**level**]] | **telnet** [**level** | **ssh** [**level**]] }
服务类型为 lan-access 用户的属性设置	**attribute** { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlanid* | **location** { **nas-ip** *ip-address* **port** *portnum* | **port** *portnum* } }*
取消服务类型为 lan-access 用户的属性设置	**undo attribute** { **ip** | **mac** | **idle-cut** | **access-limit** | **vlan** | **location** }*

2.2.5 强制切断用户连接

在某些时候，可能有必要强制切断某个或某类用户的连接。系统提供了下面的命令以实现这个目的。

请在系统视图下进行下列配置。

表2-6 强制切断用户连接

操作	命令
强制切断用户连接	**cut connection** { **all** | **access-type** { **dot1x** | **gcm** } | **domain** *domain-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name* }

2.3 RADIUS 协议配置

Quidway 系列以太网交换机的 RADIUS 协议配置，是以 RADIUS 服务器组为单位进行的。一个 RADIUS 服务器组在实际组网环境中既可以是一台独立的 RADIUS 服务器，也可以是两台配置相同、但 IP 地址不同的主、备 RADIUS 服务器。由于存在上述情况，因此每个 RADIUS 服务器组的属性包括：主服务器的 IP 地址、备份服务器的 IP 地址、共享密钥以及 RADIUS 服务器类型等。

实际上，RADIUS 协议配置仅仅定义了 NAS 和 RADIUS Server 之间进行信息交互所必须的一些参数。为了使这些参数能够生效，还必须在某个 ISP 域视图下指定该域引用配置有上述参数的 RADIUS 服务器组。具体配置命令的细节，请参见前述的“AAA 配置”一节。

RADIUS 协议的配置包括：

- 创建/删除 RADIUS 服务器组
- 设置 RADIUS 服务器的 IP 地址和端口号
- 设置 RADIUS 报文的加密密钥
- 设置 RADIUS 服务器响应超时定时器
- 设置 RADIUS 请求报文的最大传送次数
- 打开 RADIUS 计费可选开关
- 设置实时计费间隔
- 设置允许实时计费请求无响应的最大次数
- 使能停止计费报文缓存功能
- 设置停止计费请求报文的最大发送次数
- 设置支持何种类型的 RADIUS 服务器
- 设置 RADIUS 服务器的状态
- 设置发送给 RADIUS 服务器的用户名格式
- 设置发送给 RADIUS 服务器的数据流的单位
- 配置本机 RADIUS 服务器组

在以上的配置任务中，创建 RADIUS 服务器组、设置 RADIUS 服务器的 IP 地址是必需的；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.3.1 创建/删除 RADIUS 服务器组

如前所述，RADIUS 协议的配置是以 RADIUS 服务器组为单位进行的。因此，在进行其它 RADIUS 协议配置之前，必须先创建 RADIUS 服务器组并进入其视图。

可以使用下面命令创建/删除 RADIUS 服务器组。

请在系统视图下进行下列配置。

表2-7 创建/删除 RADIUS 服务器组

操作	命令
创建 RADIUS 服务器组并进入其视图	**radius scheme** *radius-server-name*
删除 RADIUS 服务器组	**undo radius scheme** *radius-server-name*

缺省情况下，系统中已创建了一个名为“system”的 RADIUS 服务器组，其各项属性均为缺省值。

一个 RADIUS 服务器组可以同时被多个 ISP 域引用。包括系统缺省创建的“System”服务器组在内，用户最多能够配置 16 个 RADIUS 服务器组。

2.3.2 设置 RADIUS 服务器的 IP 地址和端口号

当创建一个新的 RADIUS 服务器组之后，需要对属于此服务器组的 RADIUS 服务器的 IP 地址和 UDP 端口号进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和备份服务器的区别，因此最多可以设置 4 组 IP 地址和 UDP 端口号。不过，至少必须配置一个认证/授权服务器和一个计费服务器，以保证认证/授权和计费工作能够进行。

可以使用下面命令设置 RADIUS 服务器的 IP 地址和端口号。

请在 RADIUS 服务器组视图下进行下列配置。

表2-8 设置 RADIUS 服务器的 IP 地址和端口号

操作	命令
设置主 RADIUS 认证/授权或计费服务器的 IP 地址和端口号	**primary** { **accountig | authenticaiton** } *ip-address* [*port-number*]
将主 RADIUS 认证/授权或计费服务器的 IP 地址和端口号恢复为缺省值	**undo primary** { **accounting | authentication** }
设置备份 RADIUS 认证/授权或计费服务器的 IP 地址和端口号	**secondary** { **accounting** | **authentication** } *ip-address* [*port-number*]
将备份 RADIUS 认证/授权或计费服务器的 IP 地址和端口号恢复为缺省值	**undo secondary** { **accounting | authentication** }

在实际组网环境中，上述参数的设置需要根据具体需求来决定。例如：可以指定 4 组不同的数据以映射 4 台不同的 RADIUS 服务器；也可以指定两台服务器互为认证/授权和计费服务的主、备（即 A 作为主认证/授权服务器和备份计费服务器、B 作为备份认证/授权服务器和主计费服务器）；当然，也可以把这 4 组数据设置得完全一样，使其对应的服务器既作为认证/授权服务器，又作为计费服务器；同时，既作为主服务器，又作为备份服务器。

为了保证 NAS 与 RADIUS 服务器能够正常交互，在设置 RADIUS 服务器的 IP 地址和 UDP 端口之前，必须确保 RADIUS 服务器与 NAS 的路由连接正常。此外，由于 RADIUS 协议采用不同的 UDP 端口来收发认证/授权和计费报文，因此必须将认证/授权端口号和计费端口号设置得不同。RFC2138/2139 中建议的认证/授权端口号为 1812、计费端口号为 1813，但是也可以不选用 RFC 建议值（尤其是比较早期的 RADIUS Server，普遍采用 1645 作为认证/授权端口号、1646 作为计费端口号）。

在使用中，请保证 Quidway 系列以太网交换机上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。一般情况下 RADIUS 服务器的计费端口号为 1813，认证/授权端口号为 1812。

缺省情况下，主、备认证/授权和计费服务器的 IP 地址均为 0.0.0.0；其认证/授权服务的 UDP 端口号为 1812，计费服务的 UDP 端口号为 1813。

2.3.3 设置 RADIUS 报文的加密密钥

RADIUS 客户端（即交换机系统）与 RADIUS 服务器使用 MD5 算法来加密 RADIUS 报文，双方通过设置加密密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。

可以使用下面命令设置 RADIUS 报文的加密密钥。

请在 RADIUS 服务器组视图下进行下列配置。

表2-9 设置 RADIUS 报文的加密密钥

操作	命令
设置 RADIUS 认证/授权报文的加密密钥	**key authentication** *string*
恢复 RADIUS 认证/授权报文加密密钥为缺省	**undo key authentication**
设置 RADIUS 计费报文的加密密钥	**key accounting** *string*
恢复 RADIUS 计费报文加密密钥为缺省	**undo key accounting**

缺省情况下，RADIUS 认证/授权报文和 RADIUS 计费报文的加密密钥均为“huawei”。

2.3.4 设置 RADIUS 服务器响应超时定时器

如果在 RADIUS 请求报文（认证/授权请求或计费请求）传送出去一段时间后，NAS 还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户确实能够得到 RADIUS 服务。

可以使用下面命令设置 RADIUS 服务器响应超时定时器。

请在 RADIUS 服务器组视图下进行下列配置。

表2-10 设置 RADIUS 服务器响应超时定时器

操作	命令
设置 RADIUS 服务器响应超时定时器	**timer** *second*
将 RADIUS 服务器响应超时定时器恢复为缺省值	**undo timer**

缺省情况下，RADIUS 服务器响应超时定时器为 3 秒。

2.3.5 设置 RADIUS 请求报文的最大传送次数

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果 RADIUS 服务器在响应超时定时器规定的时长内没有响应 NAS，则 NAS 有必要向 RADIUS 服务器重传 RADIUS 请求报文。如果累计的传送次数超过最大传送次数而 RADIUS 服务器仍旧没有响应，则 NAS 将认为其与当前 RADIUS 服务器的通信已经中断，并将转而向其它的 RADIUS 服务器发送请求报文。

可以使用下面命令设置 RADIUS 请求报文的最大传送次数。

请在 RADIUS 服务器组视图下进行下列配置。

表2-11 设置 RADIUS 请求报文的最大传送次数

操作	命令
设置 RADIUS 请求报文的最大传送次数	**retry** *retry-times*
将 RADIUS 请求报文的最大传送次数恢复为缺省值	**undo retry**

缺省情况下，RADIUS 请求报文的最大传送次数为 3 次。

2.3.6 打开 RADIUS 计费可选开关

如果配置了此任务，交换机在对用户上线计费时如果发现没有可用的 RADIUS 计费服务器或与 RADIUS 计费服务器通信失败时，用户仍可以继续使用网络资源；否则用户将被切断。

请在 RADIUS 服务器组视图下进行下列配置。

表2-12 打开 RADIUS 计费可选开关

操作	命令
打开 RADIUS 计费可选开关	**accounting optional**
关闭 RADIUS 计费可选开关	**undo accounting optional**

缺省情况下，关闭 RADIUS 计费可选开关。

2.3.7 设置实时计费间隔

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 RADIUS 服务器发送一次在线用户的计费信息。

可以使用下面命令设置实时计费间隔。

请在 RADIUS 服务器组视图下进行下列配置。

表2-13 设置实时计费间隔

操作	命令
设置实时计费间隔	**timer realtime-accounting** *minute*
将实时计费间隔恢复为缺省值	**undo timer realtime-accounting**

其中，*minute* 为实时计费间隔时间，单位为分钟，其取值必须为 3 的整数倍。

实时计费间隔的取值对 NAS 和 RADIUS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 RADIUS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表2-14 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
≥1000	≥15

缺省情况下，实时计费间隔为 12 分钟。

2.3.8 设置允许实时计费请求无响应的最大次数

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器长时间收不到 NAS 传来的实时计费报文，它会认为线路或设备故障并停止对用户计费。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下在 NAS 端尽量与 RADIUS 服务器同步切断用户连接。Quidway 系列以太网交换机提供对连续实时计费请求无响应次数限制的设置——在 NAS 向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过所设定的限度时，NAS 将切断用户连接。

可以使用下面的命令设置允许实时计费请求无响应的最大次数。

请在 RADIUS 服务器组视图下进行下列配置。

表2-15 设置允许实时计费请求无响应的最大次数

操作	命令
设置允许实时计费请求无响应的最大次数	**retry realtime-accounting** *retry-times*
恢复允许实时计费请求无响应的最大次数为缺省值	**undo retry realtime-accounting**

考虑一下该值如何计算：假设 RADIUS 服务器的连接超时时长为 T，NAS 的实时计费间隔为 t，则 NAS 的 *count* 应取为 T 除以 t 后取整的数值。因此，在实际应用中，应尽量将 T 设置为一个能被 t 整除的数。

缺省情况下，最多允许 5 次实时计费请求无响应。

2.3.9 使能停止计费报文缓存功能

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对 Quidway 系列以太网交换机发出的停止计费请求报文没有响应，以太网交换机应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。可以使用下面的命令来设置交换机允许停止计费报文缓存功能。

请在 RADIUS 服务器组视图下进行下列配置。

表2-16 设置使能停止计费报文缓存功能

操作	命令
使能停止计费报文缓存功能	**stop-accounting-buffer enable**
关闭停止计费报文缓存功能	**undo stop-accounting-buffer enable**

缺省情况下，使能停止计费报文缓存功能。

2.3.10 停止计费报文最大重发次数设置

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对 Quidway 系列以太网交换机发出的停止计费请求报文没有响应，以太网交换机应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。可以使用下面的命令来设置缓存后的报文的最大重发次数。

请在 RADIUS 服务器组视图下进行下列配置。

表2-17 停止计费报文最大重发次数

操作	命令
停止计费报文最大重发次数	**retry stop-accounting** *retry-times*
恢复停止计费报文最大重发次数为缺省值	**undo retry stop-accounting**

缺省情况下，最多可以将缓存的停止计费请求报文重发 500 次。

2.3.11 设置支持何种类型的 RADIUS 服务器

Quidway 系列以太网交换机同时支持标准的 RADIUS 协议和华为公司自行开发的 IP Hotel、201+、Portal 等扩展 RADIUS 业务平台。

可以使用下面的命令来选择支持何种 RADIUS 服务器类型。

请在 RADIUS 服务器组视图下进行下列配置。

表2-18 设置支持何种类型的 RADIUS 服务器

操作	命令
设置支持何种类型的 RADIUS 服务器	**server-type** { **huawei** | **iphotel** | **portal** | **standard** }
恢复 RADIUS 服务器类型为缺省设置	**undo server-type**

缺省情况下，RADIUS 服务器的类型为 **standard**。

2.3.12 设置 RADIUS 服务器的状态

对于某个 RADIUS 服务器组中的主、备服务器（无论是认证/授权服务器还是计费服务器），当主服务器因故障与 NAS 的通信中断时，NAS 会主动地转而与备份服务器交互报文。当主服务器恢复正常后，NAS 却不会立即恢复与其通信，而是继续与备份服务器通信；直到备份服务器也出现故障后，NAS 才能再转而恢复与主服务器交互报文。为了使 NAS 在主服务器故障排除后迅速恢复与其通信，需要通过下面的命令手工将主服务器的状态设为 **active**。

当主服务器与备份服务器的状态都为 **active** 或都为 **block** 时，NAS 将只把报文发送到主服务器上。

请在 RADIUS 服务器组视图下进行下列配置。

表2-19 设置 RADIUS 服务器的状态

操作	命令
设置主 RADIUS 认证/授权服务器的状态	**state primary authentication** { **block** | **active** }
设置主 RADIUS 计费服务器的状态	**state primary accounting** { **block** | **active** }
设置备份 RADIUS 认证/授权服务器的状态	**state secondary authentication** { **block** | **active** }
设置备份 RADIUS 计费服务器的状态	**state secondary accounting** { **block** | **active** }

缺省情况下，RADIUS 服务器组中各 RADIUS 服务器的状态均为 **active**。

2.3.13 设置发送给 RADIUS 服务器的用户名格式

如前所述，接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，Quidway 系列以太网交换机就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，Quidway 系列以太网交换机提供下面的命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

表2-20 设置发送给 RADIUS 服务器的用户名格式

操作	命令
设置发送给 RADIUS 服务器的用户名格式	**user-name-format** { **with-domain** | **without-domain** }

📖 **说明：**

如果指定某个 RADIUS 服务器组不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 RADIUS 服务器组，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

缺省情况下，RADIUS 服务器组默认：发送给 RADIUS 服务器的用户名携带有 ISP 域名。

2.3.14 设置发送给 RADIUS 服务器的数据流的单位

Quidway 系列以太网交换机提供下面的命令以指定发送给 RADIUS 服务器的数据流的单位。

表2-21 设置发送给 RADIUS 服务器的数据流的单位

操作	命令
设置发送给 RADIUS 服务器的数据流的单位	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega- packet** | **one-packet** }
恢复发送到 RADIUS 服务器的数据流的单位为缺省设置	**undo data-flow-format**

缺省情况下，RADIUS 服务器组默认的发送数据单位为 byte，数据包的单位为 one packet。

2.3.15 配置本机 RADIUS 服务器组

华为 Quidway 系列交换机除了支持如前所述的传统的作为 RADIUS 客户端的服务——即分别采用认证/授权服务器、计费服务器的方式进行用户的认证管理外，还提供了本机的简单 RADIUS 服务器端功能（包括认证和授权），称之为本机 RADIUS 服务器功能，Quidway 系列交换机最多可以支持 16 个本机 RADIUS 服务器组。

可以使用下面命令来配置本机 RADIUS 服务器。

请在系统视图下进行下列配置。

表2-22 配置本机 RADIUS 服务器

操作	命令
创建本机 RADIUS 服务器	**local-sever nas-ip** *ip-address* **key** *password*
删除本机 RADIUS 服务器	**undo local-server nas-ip** *ip-address.*

缺省情况下，本机 RADIUS 服务器组默认的 IP 地址为 127.0.0.1，默认的密码为 huawei。

需要注意的是，采用华为公司的本机 RADIUS 服务器功能时，认证服务的 UDP 端口号为 1645，授权服务的 UDP 端口号为 1646。

2.4 AAA 和 RADIUS 协议的显示和调试

完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 AAA、RADIUS 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可清除 AAA、RADIUS 相关配置。

在用户视图下，执行 **debugging** 命令可对 AAA、RADIUS 进行调试。

表2-23 AAA 和 RADIUS 协议的显示和调试

操作	命令
显示所有或指定 ISP 域的配置信息	**display domain** [*isp-name*]
显示用户连接的相关信息	**display connection** [**access-type** { **dot1x** | **gcm** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name*]
显示本地用户的相关信息	**display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **service-type** { **telnet** | **ftp** | **lan-access** | **ssh** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlanid*]
显示本机 RADIUS 服务器组的相关信息	**display local-server statistics**
显示所有或指定 RADIUS 服务器组的配置信息	**display radius** [*radius-server-name*]
显示 RADIUS 报文的统计信息	**display radius statistics**
显示缓存的没有得到响应的停止计费请求报文	**display stop-accounting-buffer** { **radius-scheme** *radius-server-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
打开 RADIUS 报文调试开关	**debugging radius packet**
关闭 RADIUS 报文调试开关	**undo debugging radius packet**
打开本机 RADIUS 服务器组调试开关	**debugging local-server** { **all** | **error** | **event** | **packet** }
关闭本机 RADIUS 服务器组调试开关	**undo debugging local-server** { **all** | **error** | **event** | **packet** }

2.5 AAA 和 RADIUS 协议典型配置举例

AAA/RADIUS 协议与 802.1x 协议配合使用的例子，请参见“802.1x 配置”一章的“典型配置举例”部分，此处不再赘述。

2.5.1 FTP/Telnet 用户远端 RADIUS 服务器认证配置

📖 **说明：**

Telnet 用户与 FTP 用户的远端服务器认证配置方法类似，下面描述以 Telnet 用户的远端认证为例。

1. 组网需求

如下图所示的环境中，现需要通过对交换机的配置实现 RADIUS 服务器对登录交换机的 Telnet 用户的远端认证。

其中：由一台 RADIUS 服务器（其担当认证 RADIUS 服务器的职责）与交换机相连，服务器 IP 地址为 10.110.91.146，设置交换机与认证 RADIUS 服务器交互报文时的加密密码为“expert”，设置交换机从用户名中去除用户域名后再将之传给 RADIUS 服务器。

2. 组网图

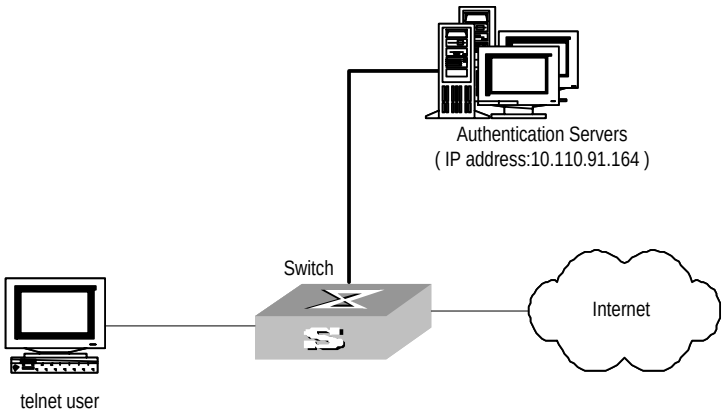


图2-2 配置 Telnet 用户的远端 RADIUS 认证

3. 配置步骤

添加 Telnet 用户。

此处略。

📖 说明：

FTP、Telnet 用户的一些配置请参考《Quidway S5000 系列以太网交换机 操作手册》的“入门操作”部分“用户界面配置”相关内容。

配置 Telnet 用户采用远端认证方式，即 scheme 方式。

[Quidway-ui-vty0-4] authentication-mode scheme

配置 domain。

[Quidway] domain cams

[Quidway-isp-cams] quit

配置 RADIUS 方案。

[Quidway] radius scheme cams

[Quidway-radius-cams] primary authentication 10.110.91.146 1812

[Quidway-radius-cams] key authentication expert

[Quidway-radius-cams] server-type Huawei

[Quidway-radius-cams] user-name-format without-domain

配置 domain 和 RADIUS 的关联。

[Quidway-radius-cams] quit

[Quidway] domain cams

[Quidway-isp-cams] radius-scheme cams

2.5.2 FTP/Telnet 用户本地 RADIUS 服务器认证配置

Telnet/FTP 用户的本地 RADIUS 认证方法与 2.5.1 小节中的远端 RADIUS 认证方法类似，只需要将 2.5.1 小节中“配置 RADIUS 方案”中的服务器 IP 地址修改为 127.0.0.1，认证密码修改为 huawei，认证服务的 UDP 端口号修改为 1645。

🕮 **说明：**

Telnet/FTP 用户的本地 RADIUS 认证的一些知识，可参考“2.3.14 配置本机 RADIUS 服务器组”的相关内容。

2.6 AAA 和 RADIUS 协议故障的诊断与排除

RADIUS 协议在 TCP/IP 协议族中处于应用层，它主要规定 NAS 与 ISP 的 RADIUS 服务器间如何交互用户信息，因此它失效的可能性比较大。

- 故障之一：用户认证/授权总是失败

故障排除：

(1) 用户名不是“userid@isp-name”的形式，或 NAS 没有指定缺省的 ISP 域——请使用正确形式的用户名或在 NAS 中设定缺省的 ISP 域。

(2) RADIUS 服务器的数据库中没有配置该用户——检查 RADIUS 服务器的数据库以保证该用户的配置信息确实存在。

(3) 用户侧输入的密码不正确——请保证接入用户输入正确的密码。

(4) RADIUS 服务器和 NAS 的报文加密密码不同——请仔细比较两端的加密密钥，确保它们相同。

(5) NAS 与 RADIUS 服务器之间存在通信故障（可以通过在 NAS 上 ping RADIUS 服务器来检查）——请保证 NAS 与 RADIUS 服务器之间能够正常通信。

- 故障之二：RADIUS 报文无法传送到 RADIUS 服务器

故障排除：

(1) NAS 与 RADIUS 服务器之间的通信线路不通（物理层/链路层）——请保证线路通畅。

(2) NAS 上没有设置相应的 RADIUS 服务器 IP 地址——请保证正确设置 RADIUS 服务器的 IP 地址。

(3) 认证/授权和计费服务的 UDP 端口设置得不正确——请保证与 RADIUS 服务器提供的端口号一致。

- 故障之三：用户认证通过并获得授权，但是不能向 RADIUS 服务器传送计费话单。

故障排除：

(1) 计费端口号设置得不正确——请正确设置 RADIUS 计费端口号。

(2) 计费服务器和认证/授权服务器不是同一台机器，NAS 却要求认证/授权和计费在同一个服务器（IP 地址相同）——请保证 NAS 的认证/授权和计费服务器的设置与实际情况相同。

第3章 HABP 特性配置

3.1 HABP 特性简介

如果交换机上配置了 802.1x，802.1x 会对启动了 802.1x 的端口进行授权认证，只允许经过授权的端口转发报文。此时如果连接交换机的端口没有进行 802.1x 的授权和认证，所有的报文将会被 802.1x 特性过滤，使用户无法对下挂的交换机进行管理。HABP(Huawei Authentication Bypass Protocol)特性可以解决这个问题。

HABP 报文携带下挂交换机的 MAC 地址等信息。交换机上启动了 HABP 特性之后，HABP 报文将会忽略端口上的 802.1x 认证，在交换机之间进行通信，从而使管理设备可以获取下挂交换机的MAC地址，对下挂的交换机进行管理。

HABP 包括 HABP Server 和 HABP Client。一般情况下，Server 会定期向 Client 发送 HABP 请求报文，收集下挂交换机的 MAC 地址。而 Client 会对请求报文进行应答，同时向下层交换机转发 HABP 请求报文。HABP Server 一般应该在管理设备上启动，HABP client 应该在下挂的交换机上启动。

如果交换机上启动了 802.1x，最好启动 HABP 特性，以便于对交换机的管理。

3.2 HABP 特性配置

HABP 特性的配置包括：

- 配置 HABP Server
- 配置 HABP Client

3.2.1 配置 HABP Server

启动了 HABP server 以后，管理设备就会向下挂的交换机发送 HABP 请求报文，收集下挂交换机的 MAC 地址，以方便对下挂交换机的管理。发送 HABP 请求报文的时间间隔也是在管理设备上进行配置的。

配置 HABP server 包括以下步骤：

1 启动 HABP 特性；

2 配置 HABP server；

3 设置发送 HABP 请求报文的时间间隔。

请在系统视图下进行下列配置。

表3-1 HABP Server 的配置

操作	命令
使能 HABP 特性	**habp enable**
恢复 HABP 特性为缺省情况	**undo habp enable**
配置当前交换机为 HABP Server	**habp server vlan** *vlan-id*
删除 HABP Server 的配置	**undo habp server**
配置发送 HABP 请求报文的时间间隔	**habp timer** *interval*
恢复发送 HABP 请求报文的时间间隔为缺省值	**undo habp timer**

缺省情况下，交换机不启动 HABP 特性。

在交换机上启动了 HABP 特性之后，缺省情况下，交换机的 HABP 特性工作在 Client 模式下。

缺省情况下，交换机发送 HABP 请求报文的时间间隔为 20 秒。

3.2.2 配置 HABP Client

HABP Client 在下挂的交换机上启动。交换机上启动 HABP 特性后，交换机缺省情况下就运行在 HABP Client 模式下。因此本配置只要在交换机上启动 HABP 特性即可。

请在系统视图下进行下列配置。

表3-2 配置 HABP Client

操作	命令
使能 HABP 特性	**habp enable**
恢复 HABP 特性为缺省情况	**undo habp enable**

缺省情况下，交换机上不启动 HABP 特性。

3.3 HABP 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令都可以显示配置后 HABP 特性的运行情况。用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可以对 HABP 模块进行调试。

表3-3 HABP 显示和调试

操作	命令
显示 HABP 特性的配置信息和状态	**display habp**
显示 HABP 的 MAC 地址表的信息	**display habp table**
显示 HABP 报文的统计信息	**display habp traffic**
显示 HABP 的调试开关状态	**display debugging habp**
打开 HABP 的调试开关	**debugging habp**
关闭 HABP 的调试开关	**undo debugging habp**

目 录

第1章 ARP 配置

1.1 ARP 简介

ARP（Address Resolution Protocol）用于将 IP 地址解析为 MAC 地址。

1. ARP 地址解析的必要性

IP 地址不能直接用来进行通信，因为网络设备只能识别 MAC 地址。IP 地址只是主机在网络层中的地址，如果要将网络层中传送的数据报交给目的主机，必须知道该主机的 MAC 地址。因此必须将 IP 地址解析为 MAC 地址。

2. ARP 地址解析的实现过程

以太网上的两台主机需要通信时，双方必须知道对方的 MAC 地址。每台主机都要维护 IP 地址到 MAC 地址的转换表，称为 ARP 映射表。ARP 映射表中存放着最近用到的一系列与本主机通信的其他主机的 IP 地址和 MAC 地址的映射。在主机启动时，ARP 映射表为空；当一条动态 ARP 映射表项规定时间没有使用时，主机将其从 ARP 映射表中删除掉，以便节省内存空间和 ARP 映射表的查找时间。

假设主机 A 和主机 B 在同一个网段，主机 A 的 IP 地址为 IP_A，B 的 IP 地址为 IP_B，主机 A 要向主机 B 发送信息。主机 A 首先查看自己的 ARP 映射表，确定其中是否包含有 IP_B 对应的 ARP 映射表项。如果找到了对应的 MAC 地址，则主机 A 直接利用 ARP 映射表中的 MAC 地址，对 IP 数据包进行帧封装，并将数据发送给主机 B；如果在 ARP 映射表中找不到对应的 MAC 地址，则主机 A 将该数据包放入 ARP 发送等待队列，然后创建一个 ARP request，并以广播方式在以太网上发送。ARP request 数据包中包含有主机 B 的 IP 地址，以及主机 A 的 IP 地址和 MAC 地址。由于 ARP request 数据包以广播方式发送，该网段上的所有主机都可以接收到该请求，但只有被请求的主机（即主机 B）会对该请求进行处理。主机 B 首先把 ARP request 数据包中的请求发起者（即主机 A）的 IP 地址和 MAC 地址存入自己的 ARP 映射表中。然后主机 B 组织 ARP 响应数据包，在数据包中填入主机 B 的 MAC 地址，发送给主机 A。这个响应不再以广播形式发送，而是直接发送给主机 A。主机 A 收到响应数据包后，提取出主机 B 的 IP 地址及其对应的 MAC 地址，加入到自己的 ARP 映射表中，并把放在发送等待队列中的发往主机 B 的所有数据包都发送出去。

一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。

1.2 ARP 配置

ARP 映射表既可以动态维护，也可以手工维护。通常将用户手工配置的 IP 地址到 MAC 地址的映射，称之为静态 ARP。通过相关的手工维护命令，用户可以显示、增加、删除 ARP 映射表中的映射项。

ARP 配置包括：

- 手工添加/删除静态 ARP 映射项
- 配置动态 ARP 老化定时器的时间

1.2.1 手工添加/删除静态 ARP 映射项

请在系统视图下进行下列配置。

表1-1 手工添加/删除静态 ARP 映射项

操作	命令
手工添加静态 ARP 映射项	**arp static** *ip-address mac-address* [*vlan-id* { *interface_type interface_num* | *interface_name* }]
手工删除静态 ARP 映射项	**undo arp** *ip-address*

需要注意的是：

- 静态ARP映射项在以太网交换机正常工作时间一直有效，但如果某ARP映射项所对应的 VLAN 被删除，则该 ARP 表项也被删除。动态 ARP 映射项的缺省有效时间为 20 分钟。
- 参数 *vlan-id* 必须是用户已经创建好的 VLAN 的 ID，且 *vlan-id* 参数后面指定的以太网端口必须属于这个 VLAN。

缺省情况下，系统 ARP 映射表缺省为空，由动态 ARP 协议获取地址映射。

1.2.2 配置动态 ARP 老化定时器的时间

为了方便用户灵活配置，系统提供以下命令允许用户指定动态 ARP 老化定时器的时间，当系统学习到一个动态 ARP 表项时，它的老化时间点以当前配置的老化时间计算。

请在系统视图下进行下列配置。

表1-2 动态 ARP 老化定时器的时间配置

操作	命令
配置动态 ARP 老化定时器的时间	**arp timer aging** *aging-time*
恢复动态 ARP 老化定时器的时间为缺省值	**undo arp timer aging**

缺省情况下，动态 ARP 老化定时器为 20 分钟。

1.3 ARP 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 ARP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **reset** 命令清除 ARP 映射项；执行 **debugging** 命令对 ARP 进行调试。

表1-3 ARP 的显示和调试

操作	命令
查看 ARP 映射表	**display arp** [**static** | **dynamic** | *ip-address*]
查看动态 ARP 老化定时器的时间	**display arp timer aging**
清除 ARP 映射项	**reset arp** [**dynamic** | **static** | **interface** { *interface_type interface_num* | *interface_name* }]
打开 ARP 调试信息开关	**debugging arp packet**
关闭 ARP 调试信息开关	**undo debugging arp packet**

第2章 DHCP-Snooping 配置

2.1 DHCP-Snooping 简介

出于安全性的考虑，可能需要记录用户上网时所用的 IP 地址，确认用户申请的 IP 地址和用户使用的主机的 MAC 地址的对应关系。三层以太网交换机可以通过 DHCP Relay 记录用户获取的 IP 地址信息，而二层交换机采取监听 DHCP 广播报文的方法来记录用户获取的 IP 地址信息。

在给用户分配 IP 地址时，DHCP 服务器发送 DHCPACK 报文。用户收到 DHCPACK 报文后，就可以获取到 IP 地址。监听 DHCPACK 报文是获取用户 IP 地址的一种方法。

DHCPREQUEST 报文是用户请求 DHCP 服务器为其分配地址的广播报文。用户通过 DHCPREQUEST 报文申请的 IP 地址与服务器通过 DHCPACK 报文分配给用户的 IP 地址相同。监听 DHCPREQUEST 报文是获取用户 IP 地址的另一种方法。

开启 DHCP-Snooping 功能后，以太网交换机就可以从接收到 DHCPACK 或 DHCPREQUEST 报文中提取并记录 IP 地址和 MAC 地址信息。

2.2 DHCP-Snooping 配置

DHCP-Snooping 配置包括：

- 开启/关闭交换机 DHCP-Snooping 功能

2.2.1 开启/关闭交换机 DHCP-Snooping 功能

请在系统视图下进行下列配置。

表2-1 开启/关闭交换机 DHCP-Snooping 功能

操作	命令
开启交换机 DHCP-Snooping 功能	**dhcp-snooping**
关闭交换机 DHCP-Snooping 功能	**undo dhcp-snooping**

缺省情况下，以太网交换机的 DHCP-Snooping 功能处于关闭状态。

2.3 DHCP-Snooping 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示通过 DHCP-Snooping 记录的用户 IP 地址与 MAC 地址的对应关系。

表2-2 DHCP-Snooping 显示和调试

操作	命令
显示通过 DHCP-Snooping 记录的用户 IP 地址和 MAC 地址的对应关系	**display dhcp-snooping**

第3章 访问管理配置

3.1 访问管理简介

用户通过以太网交换机接入外部网络是一种典型的以太网接入组网方案－－外部网络与以太网交换机相连，以太网交换机与 HUB 相连，HUB 汇集数量不等的 PC。组网示意图如下：

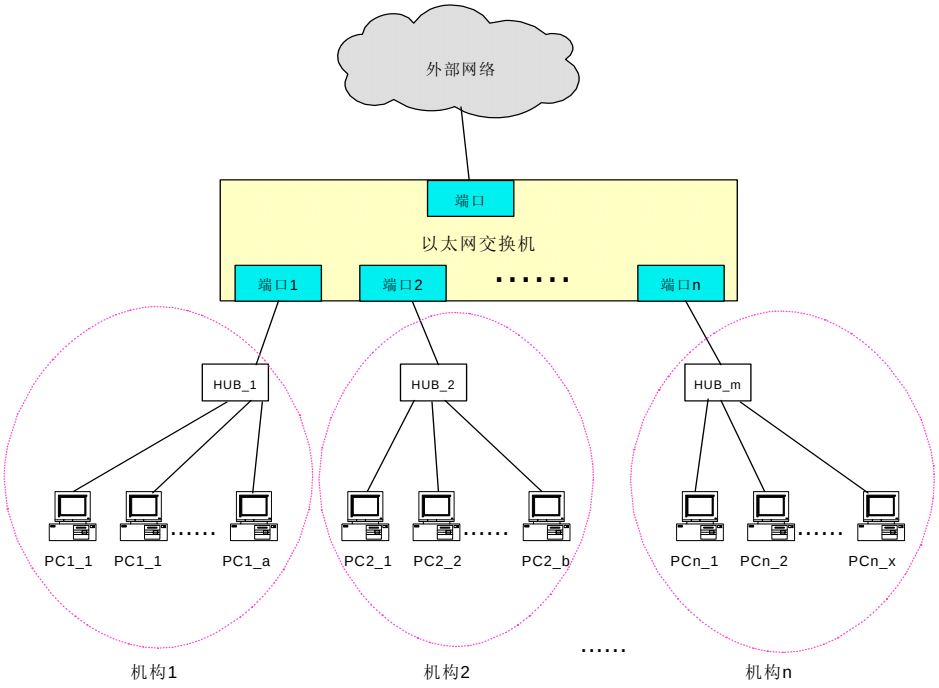


图3-1 典型的以太网接入组网图

当以太网交换机接入的用户数量不多时，从成本和安全方面的综合考虑，分配给不同企业的端口要求属于同一个VLAN，且不同企业之间不能互通。利用以太网交换机提供的端口间二层隔离功能可以实现这些需求。下面将结合 图3-1用一个实例来具体说明。

由于两个机构的网络设备处在同一个 VLAN 中，如果不采用有效的隔离措施，机构 1 内的 PC 将有可能和机构 2 中的 PC 实现互通。通过在以太网交换机的端口上配置二层隔离功能，可以控制从端口 1 发出的报文不被端口 2 接收，端口 2 发出的报文不被端口 1 接收，从而将端口 1 与端口 2 隔离开来，保证了各机构的 PC 只能与机构内的其他 PC 正常通信。

3.2 访问管理配置

访问管理的主要配置包括：

- 使能访问管理功能
- 配置端口间的二层隔离
- 开启/关闭访问管理告警开关

3.2.1 使能访问管理功能

可以通过下面的命令使能访问管理功能。只有使能访问管理功能，在各端口下配置的控制三层转发的 IP 地址池和二层隔离端口才会生效。

请在系统视图下进行下列配置。

表3-1 使能/取消访问管理功能

操作	命令
使能访问管理功能	**am enable**
关闭访问管理功能	**undo am enable**

缺省情况下，访问管理功能处于关闭状态。

3.2.2 配置端口间的二层隔离

可以通过下面的命令设置端口的二层隔离，以使该端口与某个（或某组）端口间不能进行二层转发。

请在以太网端口视图下进行下列配置。

表3-2 配置端口间的二层隔离

操作	命令
设置端口的二层隔离	**am isolate** *interface-list*
取消对指定端口的二层隔离	**undo am isolate** *interface-list*

缺省情况下，隔离端口池为空，允许该端口与所有端口进行二层转发。

3.2.3 开启/关闭告警开关

可以通过下面的命令开启访问管理告警功能。

请在系统视图下进行下列配置。

表3-3 开启/关闭访问管理告警开关

操作	命令
开启访问管理告警功能	**am trap enable**
关闭访问管理告警功能	**undo am trap enable**

缺省情况下，关闭访问控制告警功能。

3.3 访问管理显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示端口的访问控制的当前配置信息，通过查看显示信息验证配置的效果。

表3-4 显示访问控制的当前配置信息

操作	命令
显示当前的端口访问控制配置信息	**display am** [*interface-list*]

3.4 访问控制配置举例

1. 组网需求

机构 1 连接到以太网交换机的端口 1，机构 2 连接到以太网交换机的端口 2。端口 1 和端口 2 属于同一个 VLAN，机构 1 和机构 2 的设备不能互通。

2. 组网图

见 图 3-1。

3. 配置步骤

全局开启访问管理功能。

[Quidway] am enable

设置端口 1 与端口 2 二层隔离。

[Quidway-GigabitEthernet0/1] am isolate gigabitethernet0/2

第4章 IP 性能配置

4.1 IP 性能配置

IP 性能的主要配置包括：

- 配置 TCP 属性

4.1.1 配置 TCP 属性

可以配置的 TCP 属性包括：

- synwait 定时器：当发送 SYN 报文时，TCP 启动 synwait 定时器，如果 synwait 超时前未收到回应报文，则 TCP 连接将被终止。synwait 定时器的超时时间取值范围为 2～600 秒，缺省值为 75 秒。
- finwait 定时器：当 TCP 的连接状态由 FIN_WAIT_1 变为 FIN_WAIT_2 时启动 finwait 定时器，如果 finwait 定时器超时前仍未收到 FIN 报文，则 TCP 连接被终止。finwait 的取值范围为 76～3600 秒，finwait 的缺省值为 675 秒。
- 面向连接 Socket 的接收和发送缓冲区的大小：范围为 1～32K 字节，缺省值为 4K 字节。

请在系统视图下进行下列配置。

表4-1 配置 TCP 属性

操作	命令
配置 TCP 连接建立 synwait 定时器时间	**tcp timer syn-timeout** *time-value*
恢复 TCP 连接建立 synwait 定时器时间为缺省值	**undo tcp timer syn-timeout**
配置 TCP 的 FIN_WAIT_2 定时器时间	**tcp timer fin-timeout** *time-value*
恢复 TCP 的 FIN_WAIT_2 定时器时间为缺省值	**undo tcp timer fin-timeout**
配置 TCP 的 Socket 接收和发送缓冲区的大小	**tcp window** *window-size*
恢复 TCP 的 Socket 接收和发送缓冲区的大小为缺省值	**undo tcp window**

4.2 IP 性能显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 IP 性能的运行情况，通过查看显示信息验证配置的效果。在用户视图下，用户可以执行 **reset** 命令清除 IP 和 TCP 的流量统计信息；执行 **debugging** 命令对 IP 性能进行调试。

表4-2 IP 性能显示和调试

操作	命令
显示 TCP 连接状态	**display tcp status**
显示 TCP 连接统计数据	**display tcp statistics**
查看 IP 流量统计信息	**display ip statistics**
查看 ICMP 流量统计信息	**display icmp statistics**
查看系统当前套接口信息	**display ip socket** [**socktype** *sock-type*] [*task-id socket-id*]
查看 FIB 转发信息表项	**display fib**
清除 IP 流量统计信息	**reset ip statistics**
清除 TCP 流量统计信息	**reset tcp statistics**
打开 IP 调试信息开关	**debugging ip packet** [**acl** *acl-number*]
关闭 IP 调试信息开关	**undo debugging ip packet**
打开 ICMP 调试信息开关	**debugging ip icmp**
关闭 ICMP 调试信息开关	**undo debugging ip icmp**
打开 UDP 连接的调试信息	**debugging udp packet** [*task-id socket-id*]
关闭 UDP 连接的调试信息	**undo debugging udp packet** [*task-id socket-id*]
打开 TCP 调试信息开关	**debugging tcp packet** [*task-id socket-id*]
关闭 TCP 连接的调试开关	**undo debugging tcp packet** [*task-id socket-id*]
打开 TCP 事件的调试开关	**debugging tcp event** [*task-id socket-id*]
关闭 TCP 事件的调试开关	**undo debugging tcp event** [*task-id socket-id*]

4.3 IP 性能配置排错

故障现象：IP 数据报文转发正常，但 TCP 和 UDP 协议不能正常工作。

故障排除：可以打开相应的调试开关，查看调试信息。

- 通过 **display** 命令先查看 IP 性能的运行情况，并确认用户使用的电脑运行正常。
- 使用命令 **terminal debugging** 将调试信息输出到控制台上。
- 用 **debugging udp packet** 命令打开 UDP 调试开关，跟踪 UDP 的数据包。

以下为 UDP 数据报的格式：

```
UDP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
```

- 用 **debugging tcp packet** 命令打开 TCP 调试开关，跟踪 TCP 的数据包。

操作如下：

<Quidway> terminal debugging

<Quidway> debugging tcp packet

即可实时查看接收或发送的 TCP 报文，其具体报文格式如下：

```
TCP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
Sequence number :4185089
Ack number: 0
Flag  :SYN
Packet length :60
Data offset: 10
```

目 录

第1章 文件系统管理

1.1 文件系统配置

1.1.1 文件系统简介

为了方便用户对 flash 等存储设备进行有效的管理，以太网交换机提供了文件系统模块。文件系统为用户提供了文件和目录的访问管理功能，主要包括文件和目录的创建、删除、修改、更名，以及显示文件的内容等。

缺省情况下，对于有可能给用户带来损失的命令（比如删除文件、覆盖文件等），文件系统将提示用户进行确认。

根据操作对象的不同，可以把文件系统操作分为以下几类：

- 目录操作；
- 文件操作；
- 存储设备操作；
- 设置文件系统的提示方式。

1.1.2 目录操作

文件系统可以创建并删除目录、显示当前的工作目录以及指定目录下的文件或目录的信息。可以使用下面的命令来进行相应的目录操作。

请在用户视图下进行下列配置。

表1-1 目录操作

操作	命令
创建目录	**mkdir** *directory*
删除目录	**rmdir** *directory*
显示当前的工作目录	**pwd**
显示目录或文件信息	**dir** [/ **all**] [*file-url*]
改变当前目录	**cd** *directory*

1.1.3 文件操作

文件系统可以删除文件、恢复删除的文件、彻底删除文件、显示文件的内容、重新命名、拷贝文件、移动文件、显示指定的文件的信息。可以使用下面的命令来进行相应的文件操作。

请在用户视图下进行下列配置。

表1-2 文件操作

操作	命令
删除文件	**delete** [**/unreserved**] *file-url*
恢复删除文件	**undelete** *file-url*
彻底删除回收站中的文件	**reset recycle-bin** [*file-url*]
显示文件的内容	**more** *file-url*
重新命名文件	**rename** *fileurl-source fileurl-dest*
拷贝文件	**copy** *fileurl-source fileurl-dest*
移动文件	**move** *fileurl-source fileurl-dest*
显示目录或文件信息	**dir** [/ **all**] [*file-url*]

1.1.4 存储设备操作

文件系统可以格式化指定的存储设备。可以使用下面的命令来格式化指定的存储设备

请在用户视图下进行下列配置。

表1-3 存储设备操作

操作	命令
格式化存储设备	**format** *filesystem*

1.1.5 设置文件系统的提示方式

可以使用下面的命令来设置当前文件系统的提示方式。

请在系统视图下进行下列配置。

表1-4 文件系统操作

操作	命令
文件系统的提示方式	**file prompt { alert | quiet }**

1.2 配置文件管理

1.2.1 配置文件管理简介

配置文件管理模块，具有较好的用户操作界面。它以命令行文本格式保存用户对以太网交换机进行的配置，记录下用户的整个配置过程。用户可以非常方便的查阅这些配置信息。

配置文件的格式如下：

- 以命令格式保存；
- 只保存非缺省的配置参数；
- 命令的组织以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以# 开始的为注释行）。
- 文件中各节的安排顺序通常为：系统配置、物理端口配置、逻辑接口配置、路由协议配置等。
- 以 end 为结束。

配置文件管理操作包括：

- 查看以太网交换机的当前配置和起始配置；
- 修改和保存当前配置；
- 擦除 Flash Memory 中配置文件。

1.2.2 查看以太网交换机的当前配置和起始配置

以太网交换机上电时，系统从 Flash Memory 中读取配置文件，对以太网交换机进行初始化。以太网交换机上电时从 Flash Memory 中读取的配置文件被称为起始配置（saved-configuration）文件。如果 Flash Memory 中没有配置文件，则系统用缺省参数进行初始化。与起始配置相对应，系统运行过程中正在生效的配置称为当前配置（current-configuration）。可以使用下面的命令来查看以太网交换机的当前配置和起始配置。

下列配置可以在所有视图下执行。

表1-5 查看以太网交换机的配置

操作	命令
查看以太网交换机的起始配置	**display saved-configuration**
查看以太网交换机的当前配置	**display current-configuration** [**controller** | **interface** *interface-type* [*interface-number*] | **configuration** [**system** | **user-interface**]] [| { **begin** | **exclude** | **include** } *regular-expression*]

📖 **说明：**

配置文件的显示格式与保存格式相同。

1.2.3 修改和保存当前配置

用户通过命令行接口可以修改以太网交换机的当前配置。如果想将当前配置作为系统下次上电时的起始配置，请用 **save** 命令，将当前配置保存到 Flash Memory 中。

请在用户视图下进行下列配置。

表1-6 保存当前配置

操作	命令
保存当前配置	**save**

1.2.4 擦除 Flash Memory 中配置文件

可以使用 **reset saved-configuration** 命令擦除 Flash Memory 中的配置文件。配置文件被擦除后，以太网交换机下次上电时，系统将采用缺省的配置参数进行初始化。

请在用户视图下进行下列配置。

表1-7 擦除 Flash Memory 中配置文件

操作	命令
擦除 Flash Memory 中配置文件	**reset saved-configuration**

在以下几种情况下，用户可能需要擦除 Flash Memory 中配置文件：

- 在以太网交换机的软件升级之后，系统软件和配置文件不匹配。
- Flash Memory 中的配置文件被破坏（常见原因是加载了错误的配置文件）。

⚠ 注意：

使用 **delete** 命令删除文件，被删除的文件被保存在回收站中，仍会占用存储空间。如果用户经常使用 **delete** 命令删除文件（而不是彻底清除文件），则可能导致以太网交换机的存储空间不足；在这种情况下，用户需要查看回收站中是否仍有废弃文件；使用 **reset recycle-bin** 命令可以将回收站中的废弃文件彻底清除，以回收存储空间。

1.3 FTP 配置

1.3.1 FTP 简介

FTP 是 Internet 和 IP 网络上传输文件的通用方法。在万维网（WWW）出现以前，用户使用命令行方式传输文件，最通用的应用程序就是 FTP。虽然目前大多数用户在通常情况下选择使用 Email 和 Web 传输文件，但是 FTP 仍然有着比较广泛的用途。

FTP 协议在 TCP/IP 协议族中属于应用层协议，用于在远端服务器和本地主机之间传输文件。

以太网交换机提供的 FTP 服务包括：

- FTP Server 服务，用户可以运行 FTP 客户端程序登录到服务器上（接受用户登录前，网络管理员需要事先配置好 FTP Server 的 IP 地址），访问服务器上的文件。
- FTP Client 服务，用户在微机上通过终端仿真程序或 Telnet 程序建立与以太网交换机（FTP Client）的连接后，输入 ftp X.X.X.X（X.X.X.X 代表远程 FTP Server 的 IP 地址）命令，建立以太网交换机与远程 FTP Server 的连接，访问远程 FTP Server 上的文件。

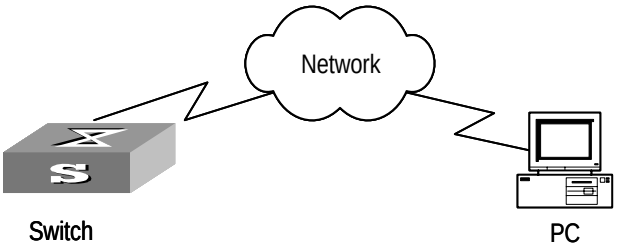


图1-1 FTP 配置示意图

交换机作为 FTP Client 时的配置。

表1-8 交换机作为 FTP Client 时的配置

设备	配置	缺省值	配置说明
Switch	可以直接使用 ftp 命令登录远端的 FTP Server	-	用户首先获取 FTP 用户命令和密码，然后登录远端的 FTP Server。这样才能取得相应目录和文件的权限。
PC	启动 FTP Server，并作了用户名、密码、用户的权限等相关的配置	-	—

交换机作为 FTP Server 时的配置。

表1-9 交换机作为 FTP Server 时的配置

设备	配置	缺省值	配置说明
Switch	启动 FTP Server 功能	缺省情况下，系统关闭 FTP 服务器。	用户可以通过 **ftp-server** 命令查看交换机上 FTP Server 功能的配置信息。
	配置 FTP 服务器的验证和授权	-	配置 FTP 用户的用户名、密码、授权的工作目录。
	配置 FTP 服务器的运行参数	-	配置 FTP 服务的超时时间
PC	使用 FTP 客户端程序登录交换机	-	—

⚠ 注意：

FTP 功能可以正常使用的条件是交换机和 PC 之间路由可达。

1.3.2 启动/关闭 FTP 服务器

可以使用下面的命令在以太网交换机上启动/关闭 FTP 服务器。请在系统视图下进行下列配置。

表1-10 启动/关闭 FTP 服务器

操作	命令
启动 FTP 服务器	**ftp server enable**
关闭 FTP 服务器	**undo ftp server**

FTP 服务器可同时支持多个用户的访问。远端 FTP 用户向 FTP 服务器发送请求，FTP 服务器执行相应的动作，并向用户返回执行的结果。

缺省情况下，系统关闭 FTP 服务器。

1.3.3 配置 FTP 服务器的验证和授权

FTP 服务器的授权信息包含提供给 FTP 用户的工作目录的路径。只有验证通过和授权成功的用户，才能享受 FTP 服务器的服务。可以使用下面的命令来进行 FTP 服务器的验证和授权配置。FTP 服务器的授权信息是提供给 FTP 用户的顶级工作目录等信息。

请在相应视图下进行下列配置。

表1-11 配置 FTP 服务器的验证和授权

操作	命令
创建新的本地 FTP 用户，并且进入本地用户配置视图（系统视图）	**local-user** *username*
删除本地 FTP 用户（系统视图）	**undo local-user** [*username* **| all** [**service-type ftp**]]
配置 FTP 用户的验证信息（本地用户视图）	**password** { **cipher**	**simple** } *password*
配置 FTP 用户的授权信息（本地用户视图）	**service-type ftp ftp-directory** *directory*
取消 FTP 用户的验证信息（本地用户视图）	**undo password**
取消 FTP 用户的授权信息（本地用户视图）	**undo service-type ftp** [**ftp-directory**]

只有验证通过和授权成功的用户，才能得到 FTP 服务器的服务。

1.3.4 配置 FTP 服务器的运行参数

可以使用下面的命令来配置 FTP 服务器的连接空闲时间。为了防止未授权用户的非法入侵，如果在一定时间内没有收到 FTP 客户端发来的服务请求，FTP 服务器则断开与该 FTP 客户端的连接，这个时间就是 FTP 服务器的连接空闲时间。

请在系统视图下进行下列配置。

表1-12 配置 FTP 服务器的超时断连时间

操作	命令
配置 FTP 服务器的超时断连时间	**ftp timeout** *minute*
恢复 FTP 服务器的超时断连时间的缺省值	**undo ftp timeout**

缺省情况下，超时断连时间为 30 分钟。

1.3.5 FTP 服务器的显示和调试

在完成上述配置后，可以在所有视图下执行 **display** 命令，显示配置后 FTP 服务器的运行情况，通过查看显示信息验证配置的效果。

表1-13 FTP 服务器的显示和调试

操作	命令
查看 FTP 服务器	**display ftp-server**
查看登录的 FTP 用户	**display ftp-user**

display ftp-server 命令显示当前 FTP 服务器的配置情况，包括 FTP 服务器支持的最大用户数和超时断连时间。**display ftp-user** 显示登录的 FTP 用户的详细情况。

1.3.6 FTP 客户端介绍

FTP 客户端是以太网交换机提供给用户的一个附加功能，它是一个应用模块，不用做任何功能配置。此时，交换机作为 FTP 客户端与远程服务器连接，并键入 FTP 客户端的命令来进行相应的操作（如建立、删除目录等）。

1.3.7　交换机作为 FTP Client 实现配置文件的备份和和软件升级配置举例

1. 组网需求

交换机作为 FTP Client，远端的 PC 作为 FTP Server，在 FTP Server 上作了如下配置：配置了一个 FTP 用户名为 switch，密码为 hello，对该用户授权了 PC 机上 Switch 目录的读写权限。交换机上的一个 VLAN 接口的 IP 地址为 1.1.1.1，PC 的 IP 地址为 2.2.2.2，交换机和 PC 之间路由可达。

交换机的应用程序 switch.app 保存在 PC 上。交换机通过 FTP 从远端的 FTP Server 上下载 switch.app，同时将交换机的配置文件 config.cfg 上传到 FTP Server 的目录 switch 下实现配置文件的备份。

2. 组网图

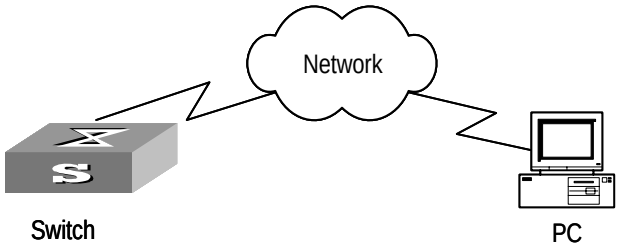


图1-2 FTP 配置示意图

3. 配置步骤

(1) 在PC上配置FTP Server的相关参数：配置了一个FTP用户名为switch，密码为 hello，对该用户授权了 PC 机上 Switch 目录的读写权限。此处不详细说明。

(2) 交换机上的配置

用户登录到交换机上。（用户可以在本地通过 Console 口登录到交换机上，也可以通过 telnet 远程登录到交换机上。各种登录方式请参见入门模块的描述。）

<Quidway>

注意：

如果交换机的 Flash memory 空间不够大，请删除 Flash 中原有的应用程序然后再下载新的应用程序到交换机的 Flash 中。

在用户视图下输入命令进行 FTP 连接，输入正确用户名和密码登录到 FTP Server。

<Quidway> ftp 2.2.2.2

```
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:*****
230 Logged in successfully
```

[ftp]

进入 FTP Server 的授权路径

[ftp] cd switch

执行 put 命令将交换机的配置文件 config.cfg 上传到 FTP Server。

[ftp] put config.cfg

执行 get 命令将 FTP Server 上的文件 switch.app 下载到交换机的 Flash。

[ftp] get switch.app

执行 quit 命令中断 FTP 连接，退回到用户视图下。

[ftp] quit

<Quidway>

用户可以通过命令 boot boot-loader 来指定下载的程序为下次启动时的应用程序，然后重启交换机，实现交换机应用程序的升级。

<Quidway> boot boot-loader switch.app

<Quidway> reboot

1.3.8 交换机作为 FTP Server 实现配置文件的备份和软件升级配置举例

1. 组网需求

交换机作为 FTP Server，远端的 PC 作为 FTP Client。在 FTP Server 上作了如下配置：配置了一个 FTP 用户名为 switch，密码为 hello，对该用户授权了交换机上 Flash 根目录的读写权限。交换机上的一个 VLAN 接口的 IP 地址为 1.1.1.1，PC 的 IP 地址为 2.2.2.2，交换机和 PC 之间路由可达。

交换机的应用程序 switch.app 保存在 PC 上。PC 通过 FTP 向远端的交换机上传 switch.app，同时将交换机的配置文件 config.cfg 下载到 PC 实现配置文件的备份。

2. 组网图

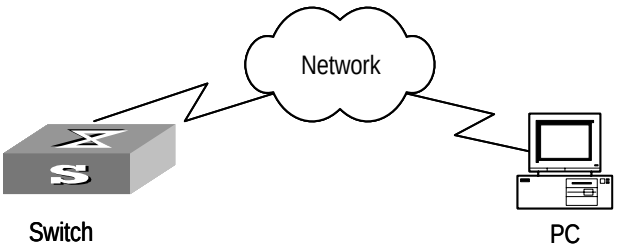


图1-3 FTP 配置示意图

3. 配置步骤

(1)　交换机上的配置

用户登录到交换机上。（用户可以在本地通过 Console 口登录到交换机上，也可以通过 telnet 远程登录到交换机上。各种登录方式请参见入门模块的描述。）

<Quidway>

在交换机上开启 FTP 服务，设置好用户名、密码和路径：

[Quidway] ftp server enable

[Quidway] local-user switch

[Quidway-luser-switch] service-type ftp ftp-directory flash:

[Quidway-luser-switch] password simple hello

(2)　在 PC 上运行 FTP Client 程序，同交换机建立 FTP 连接，同时通过上载操作把交换机的应用程序 switch.app 上载到交换机的 Flash 根目录下，同时从交换机上下载配置文件 config.cfg。FTP Client 应用程序由用户自己购买、安装，Quidway 系列交换机不附带此软件。

注意：

如果交换机的 Flash memory 空间不够大，请删除 Flash 中原有的应用程序然后再上载新的应用程序到交换机 Flash 中。

(3)　在上载完毕后，用户在交换机上进行升级操作。

<Quidway>

用户可以通过命令 boot boot-loader 来指定下载的程序为下次启动时的应用程序，然后重启交换机，实现交换机应用程序的升级。

<Quidway> boot boot-loader switch.app

<Quidway> reboot

1.4 TFTP 配置

1.4.1 TFTP 简介

TFTP（Trivial File Transfer Protocol）是一种简单文件传输协议。相对于另一种文件传输协议 FTP，TFTP 不具有复杂的交互存取接口和认证控制，适用于客户端和服务器之间不需要复杂交互的环境。TFTP 协议一般在 UDP 的基础上实现。

TFTP 协议传输是由客户端发起的。当需要下载文件时，由客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据，并向服务器发送确认；当需要上传文件时，由客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据，并接收服务器的确认。TFTP 传输文件有两种模式：一种是二进制模式，用于传输程序文件；另一种是 ASCII 码模式，用于传输文本文件。

配置 TFTP 之前，网络管理员需要首先配置好 TFTP 客户端和服务器的 IP 地址，并且确保客户端 IP 地址和服务器 IP 地址属于同一个网段。

交换机只能作为 TFTP 客户端。

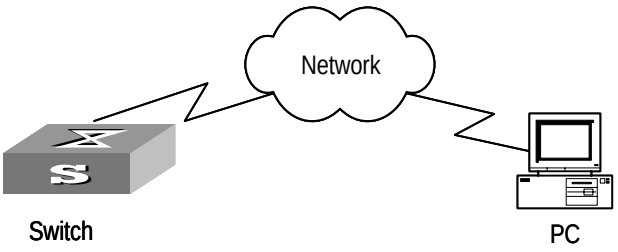


图1-4 TFTP 配置示意图

交换机作为 TFTP Client 时的配置。

表1-14　交换机作为 TFTP Client 时的配置

设备	配置	缺省值	配置说明
Switch	配置交换机 VLAN 接口的 IP 地址，使其和 TFTP Server 的 IP 地址在同一网段	-	TFTP 适用于客户端和服务器之间不需要复杂交互的环境，请保证交换机 VLAN 接口的 IP 地址和 TFTP Server 的 IP 地址在同一网段。
	可以直接使用 TFTP 命令登录远端的 TFTP Server 上传或者下载文件	-	-
PC	启动 TFTP Server，并作了 TFTP 工作目录的配置	-	—

1.4.2 配置文件传输模式

TFTP 传输文件有两种模式：一种是二进制模式，用于传输程序文件；另一种是 ASCII 码模式，用于传输文本文件。可以使用下面的命令来配置文件传输模式。

请在系统视图下进行下列配置。

表1-15　配置文件传输模式

操作	命令
设置 TFTP 的文件传输模式	**tftp** { **ascii** | **binary** }

缺省情况下，TFTP 以二进制模式传输文件。

1.4.3 用 TFTP 下载文件

当需要下载文件时，客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据，并向服务器发送确认。可以使用下面的命令利用 TFTP 下载文件。

请在系统视图下进行下列配置。

表1-16　用 TFTP 下载文件

操作	命令
用 TFTP 获取文件	**tftp get** *//X.X.X.X/ path_name1 path_name2*

配置命令中，*X.X.X.X* 参数代表 TFTP 服务器的 IP 地址；*//X.X.X.X/path_name1* 指的是要下载的 TFTP 服务器上的文件信息；

path_name2 参数代表下载后存储在交换机上的文件名。*path_name1* 和 *path_name2* 可以不同。

1.4.4 用 TFTP 上传文件

当交换机需要向 TFTP 服务器上传文件时，交换机作为客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据，并接收服务器的确认。可以使用下面的命令上传文件。

请在系统视图下进行下列配置。

表1-17 用 TFTP 上传文件

操作	命令
用 TFTP 保存文件	**tftp put** *path_name1 //X.X.X.X/path_name2*

配置命令中，*path_name1* 参数代表要上传到服务器的文件。*//X.X.X.X/path_name2* 指的是文件上传到 TFTP 服务器的存储目录；*X.X.X.X* 参数代表 TFTP 服务器的 IP 地址。

1.4.5 交换机作为 TFTP Client 实现配置文件的备份和和软件升级配置举例

1. 组网需求

交换机作为 TFTP Client，PC 作为 TFTP Server，在 TFTP Server 上配置了 TFTP 的工作路径。交换机上的一个 VLAN 接口的 IP 地址为 1.1.1.1，交换机和 PC 相连的端口属于该 VLAN，PC 的 IP 地址为 1.1.1.2。

交换机的应用程序 switch.app 保存在 PC 上。交换机通过 TFTP 从 TFTP Server 上下载 switch.app，同时将交换机的配置文件 config.cfg 上传到 TFTP Server 的工作目录实现配置文件的备份。

2. 组网图

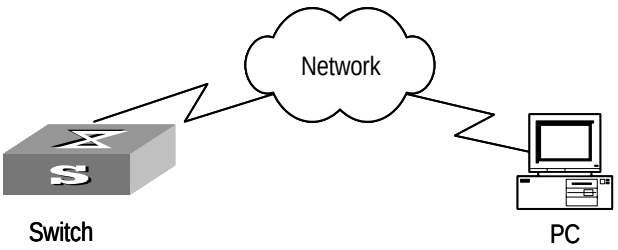


图1-5 TFTP 配置示意图

3. 配置步骤

(1)　在 PC 上启动了 TFTP Server，配置 TFTP Server 的工作目录。

(2)　交换机上的配置

用户登录到交换机上。（用户可以在本地通过 Console 口登录到交换机上，也可以通过 telnet 远程登录到交换机上。各种登录方式请参见入门模块的描述。）

<Quidway>

注意：

如果交换机的 Flash memory 空间不够大，请删除 Flash 中原有的应用程序然后再下载新的应用程序到交换机的 Flash 中。

进入系统视图。

<Quidway> system-view

[Quidway]

配置 VLAN 接口的 IP 地址为 1.1.1.1，同时保证与 PC 相连的端口属于这个 VLAN。（本例中以 VLAN 1 为例。）

[Quidway] interface vlan 1

[Quidway-vlan-interface1] ip address 1.1.1.1 255.255.255.0

[Quidway-vlan-interface1] quit

将交换机的应用程序 switch.app 从 TFTP Server 下载到交换机。

[Quidway] tftp get //1.1.1.2/switch.app switch.app

将交换机的配置文件 config.cfg 上传到 TFTP Server。

[Quidway] tftp put config.cfg //1.1.1.2/config.cfg

执行 quit 命令退回到用户视图下。

[Quidway] quit

<Quidway>

用户可以通过命令 boot boot-loader 来指定下载的程序为下次启动时的应用程序，然后重启交换机，实现交换机应用程序的升级。

<Quidway> boot boot-loader switch.app

<Quidway> reboot

第2章 MAC 地址表管理

2.1 MAC 地址表管理简介

为了快速转发报文，以太网交换机需要维护 MAC 地址表。MAC 地址表的表项包含了与以太网交换机相连的设备的MAC地址及与此设备相连的交换机的端口号。MAC 地址表中的动态表项（非手工配置）是由以太网交换机学习得来的。以太网交换机学习 MAC 地址的方法如下：如果从某端口（假设为端口 A）收到一个数据帧，以太网交换机就会分析该数据帧的源 MAC 地址（假设为 MAC-SOURCE）并认为目的 MAC 地址为 MAC-SOURCE 的报文可以由端口 A 转发；如果 MAC 地址表中已经包含 MAC-SOURCE，交换机将对应表项进行更新，如果 MAC 地址表中尚未包含 MAC-SOURCE，交换机则将这个新 MAC 地址（以及该 MAC 地址对应的转发端口）作为一个新的表项加入到 MAC 地址表中。

对于目的 MAC 地址能够在 MAC 地址表中找到的报文，系统会直接使用硬件转发；对于目的 MAC 地址不能在地址表中查到的报文，系统对报文采用广播方式进行转发。如果广播后，报文到达了目的 MAC 地址对应的网络设备，目的网络设备将应答此广播报文，应答报文中包含了此设备的 MAC 地址，以太网交换机通过地址学习将新的 MAC 地址加入到 MAC 地址转发表中。去往同一目的 MAC 地址的后续报文，就可以利用到该新增的 MAC 地址表项直接进行转发了。如果将报文广播后仍然无法找到对应的 MAC 地址，交换机则将该报文丢弃，并告知报文发送端：目的地址不可到达。

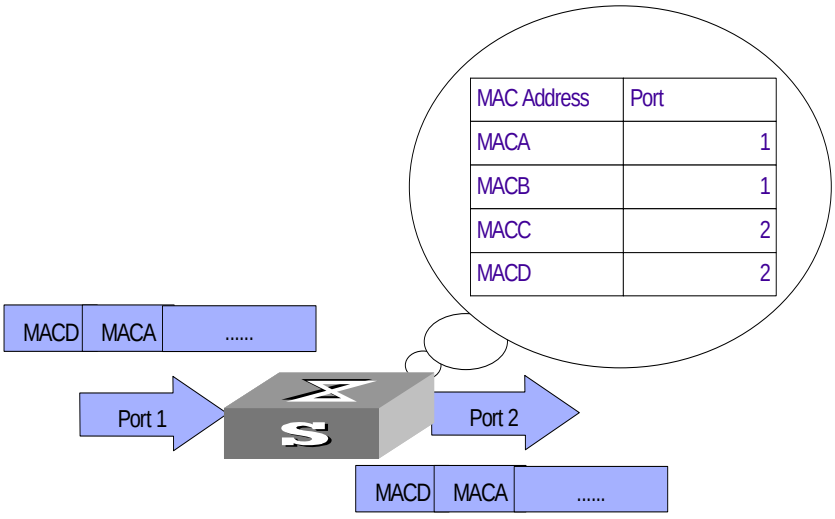


图2-1 以太网交换机利用 MAC 地址表转发报文

以太网交换机提供 MAC 地址老化的功能。如果在一定时间内没有收到来自某网络设备的报文，交换机就会把与此设备相关的 MAC 地址表项删除。MAC 地址老化对静态 MAC 地址表项无效。

用户可以根据网络实际情况人工配置（添加或修改）MAC 地址表项，添加或修改的表项可以是静态的表项或者动态的表项。

2.2 配置 MAC 地址表管理

MAC 地址表管理配置包括：

- 设置 MAC 地址表项
- 设置系统的 MAC 地址老化时间

2.2.1 设置 MAC 地址表项

管理员根据实际情况可以人工添加、修改或删除 MAC 地址表中的表项。可以删除与某个端口相关的所有 MAC 地址表项（只能是单播地址），也可以选择删除某类 MAC 地址表项如动态表项、静态表项。可以使用下面的命令来添加、修改或删除 MAC 地址表中的表项。

请在系统视图下进行下列配置。

表2-1 设置 MAC 地址表项

操作	命令
添加/修改地址表项	**mac-address** { **static** | **dynamic** } *hw-addr* **interface** { *interface-name* | *interface-type interface-num* } **vlan** *vlan-id*
删除地址表项	**undo mac-address** [**static** | **dynamic**] [[*hw-addr*] **interface** { *interface-name* | *interface-type interface-num* } **vlan** *vlan-id*]

2.2.2 设置系统 MAC 地址老化时间

设置合适的老化时间可以有效的实现 MAC 地址老化的功能。用户设置的老化时间过长或者过短，都可能导致以太网交换机广播大量找不到目的 MAC 地址的数据报文，影响交换机的运行性能。

如果用户设置的老化时间过长，以太网交换机可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致交换机无法根据网络的变化更新 MAC 地址表。如果用户设置的老化时间太短，以太网交换机可能会删除有效的的 MAC 地址表项。

请在系统视图下进行下列配置。

表2-2 设置系统 MAC 地址老化

操作	命令
设置 MAC 地址动态表项的老化时间	**mac-address timer** { **aging** *age* | **no-aging** }
恢复 MAC 地址老化时间的缺省值	**undo mac-address timer aging**

此命令为系统视图命令，作用于全部端口上。地址老化只对动态的（学习到的或者用户配置可老化的）MAC 地址表项起作用。

一般情况下，推荐使用老化时间 *age* 的缺省值 300 秒。使用参数 **no-aging** 时表示不对 MAC 地址表项进行老化。

2.2.3 设置以太网端口最多可以学习到的 MAC 地址数

以太网交换机可以利用MAC地址学习功能获取与某端口相连的网段上各网络设备的 MAC 地址。对于发往这些 MAC 地址的报文，以太网交换机可以直接使用硬件转发。如果 MAC 地址表过于庞大，可能导致以太网交换机的转发性能的下降。

通过设置以太网端口最多学习到的 MAC 地址数，用户可以控制以太网交换机维护的 MAC 地址表的表项数量。如果用户设置的值为 *count*，则该端口学习到的 MAC 地址条数达到 *count* 时，该端口将不再对 MAC 地址进行学习。

请在以太网端口视图下进行下列配置。

表2-3 设置以太网端口最多可以学习到的 MAC 地址数

操作	命令
设置以太网端口最多可以学习到的 MAC 地址数	**mac-address max-mac-count** *count*
取消对以太网端口最多可以学习到的 MAC 地址数的限制	**undo mac-address max-mac-count**

缺省情况下，交换机对于端口最多可以学习到的 MAC 地址数目没有限制。

2.3 MAC 地址表管理的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 MAC 地址表管理的运行情况，通过查看显示信息验证配置的效果。

在用户视图下用户可以执行 **debug** 命令对 MAC 地址表进行调试。

表2-4 MAC 地址表管理的显示和调试

操作	命令
显示地址表信息	**display mac-address** [*mac-addr* [**vlan** *vlan-id*] | [**static** | **dynamic**] [**interface** { *interface-name* | *interface-type interface-num* }] [**vlan** *vlan-id*] [**count**]]
显示地址表动态表项的老化时间	**display mac-address aging-time**
打开地址表管理的调试信息开关	**debugging mac-address**
关闭地址表管理的调试信息开关	**undo debugging mac-address**

2.4 MAC 地址表管理典型配置举例

1. 组网需求

用户通过 Console 口登录到交换机，配置地址表管理。要求设置地址老化时间为 500 秒，在 vlan1 中的 Ethernet 0/2 端口添加一个静态地址 00e0-fc35-dc71。

2. 组网图

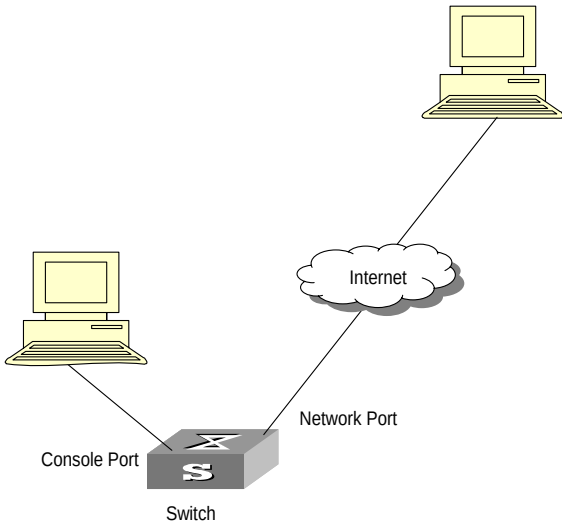


图2-2 地址表管理典型配置组网图

3. 配置步骤

进入交换机系统视图。

<Quidway> system-view

增加一个 MAC 地址（指出所属 VLAN、端口、状态）。

[Quidway] mac-address static 00e0-fc35-dc71 interface ethernet 0/2 vlan 1

地址老化时间设置为 500 秒。

[Quidway] mac-address timer aging 500

在所有视图下察看 MAC 地址配置。

[Quidway] display mac-address interface ethernet 0/2

```
MAC ADDR             VLAN ID   STATE      PORT INDEX     AGING TIME
00-e0-fc-35-dc-71    1         Static     Ethernet0/2    NOAGED
00-e0-fc-17-a7-d6    1         Learned    Ethernet0/2    AGING
00-e0-fc-5e-b1-fb    1         Learned    Ethernet0/2    AGING
00-e0-fc-55-f1-16    1         Learned    Ethernet0/2    AGING
---  4 mac address(es) found on port Ethernet0/2 ---
```

第3章 设备管理

3.1 设备管理简介

以太网交换机的设备管理功能能够向用户显示单板当前工作状态信息和事件调试信息，实现对物理设备的状态和通讯进行维护和管理。并可提供重启命令实现系统的重新启动，在系统某些功能出现故障时可以使用该命令实现系统重启。

3.2 配置设备管理

设备管理的配置任务很简单。对用户而言，主要是对设备管理进行显示和调试。

设备管理的配置任务包括：

- 复位以太网交换机
- 指定以太网交换机下次启动采用的 APP
- 升级 BootROM

3.2.1 复位以太网交换机

当以太网交换机出现故障需要重启的时候可以通过以下命令来复位。

请在用户视图下进行下列配置：

表3-1 复位以太网交换机

操作	命令
复位以太网交换机	**reboot**

3.2.2 指定以太网交换机下次启动采用的 APP

APP 指的是交换机采用的主机软件。当 Flash Memory 中有多个 APP 时，用户可以指定交换机下次启动所采用的 APP。

请在用户视图下进行下列配置：

表3-2 指定交换机下次启动采用的 APP

操作	命令
指定交换机下次启动采用的 APP	**boot boot-loader** *file-url*

3.2.3 设置单板上的温度告警阈值

当单板的温度超出一定范围时，交换机系统可以发出告警信号。

请在用户视图下进行下列配置。

表3-3 设置单板上的温度告警阈值

操作	命令
设置单板上的温度告警阈值	**temperature-limit** *slot down-value up-value*
恢复单板上的温度告警阈值为缺省值	**undo temperature-limit** *slot*

3.2.4 升级 BootROM

在系统运行过程中，用户可以使用 Flash Memory 中的 BootROM 程序升级交换机上正在运行的 BootROM。本配置任务给远程升级带来方便。用户可以在远端利用 FTP 上传 BootROM 程序到交换机，然后使用本命令升级 BootROM。

请在用户视图下进行下列配置：

表3-4 升级 BootROM

操作	命令
升级 BootROM	**boot bootrom** *file-url*

3.3 设备管理的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后设备管理的运行情况，通过查看显示信息验证配置的效果。

表3-5 设备管理的显示和调试

操作	命令
显示下次启动采用的 APP	**display boot-loader**
显示各单板的模块类型及工作状态	**display device**
显示内置风扇的工作状态	**display fan** [*fan-id*]
显示环境信息	**display environment**
显示电源状态	**display power** [*powe-ID*]
显示交换机的 CPU 使用状态	**display cpu**
显示交换机的内存使用状态	**display memory** [**slot** *slot-number*]

3.4 利用设备管理命令实现远程升级交换机配置举例

1. 组网需求

用户通过 telnet 远程登录到交换机上，从 FTP Server 上下载交换机的应用程序到交换机的 Flash，通过命令行实现交换机的远程升级。

交换机作为 FTP Client，远端的 PC 作为 FTP Server，在 FTP Server 上作了如下配置：配置了一个 FTP 用户名为 switch，密码为 hello，对该用户授权了 PC 机上 Switch 目录的读写权限。交换机上的一个 VLAN 接口的 IP 地址为 1.1.1.1，PC 的 IP 地址为 2.2.2.2，交换机和 PC 之间路由可达。

交换机的应用程序 switch.app 和 boot.app 保存在 PC 上。交换机通过 FTP 从远端的 FTP Server 上下载 switch.app 和 boot.app。

2. 组网图

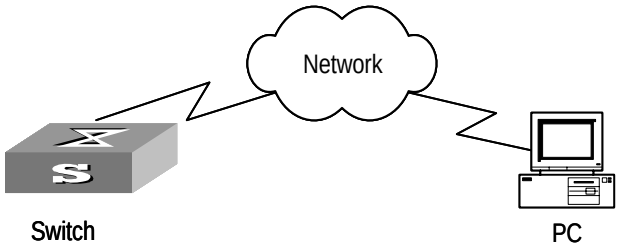


图3-1 FTP 配置示意图

3. 配置步骤

(1) 在PC上配置FTP Server的相关参数：配置了一个FTP用户名为switch，密码为 hello，对该用户授权了 PC 机上 Switch 目录的读写权限。此处不详细说明。

(2) 交换机上的配置

#交换机上已经配置了 telnet 用户的用户名为 user，级别为 3 级用户，口令为 hello，验证方式为需要进行用户名和口令的验证。

用户在 PC 上执行 telnet 命令登录到交换机上。

<Quidway>

⚠ 注意：

如果交换机的 Flash memory 空间不够大，请删除 Flash 中原有的应用程序然后再下载新的应用程序到交换机的 Flash 中。

在用户视图下输入命令进行 FTP 连接，输入正确用户名和密码登录到 FTP Server。

<Quidway> ftp 2.2.2.2

```
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:*****
230 Logged in successfully
```

[ftp]

进入 FTP Server 的授权路径

[ftp] cd switch

执行 get 命令将 FTP Server 上的文件 switch.app 和 boot.app 下载到交换机的 Flash。

[ftp] get switch.app

[ftp] get boot.app

执行 quit 命令中断 FTP 连接，退回到用户视图下。

[ftp] quit

<Quidway>

升级 BOOTROM。

<Quidway> boot bootrom boot.app

```
please wait ...
 Bootrom is updated!
```

指定下载的程序为下次启动时的应用程序，然后重启交换机，实现交换机应用程序的升级。

<Quidway> boot boot-loader switch.app

<Quidway>display boot-loader

```
The app to boot at the next time is: flash:/Switch.app
```

<Quidway> reboot

第4章　系统维护与调试

4.1　系统基本配置

系统基本配置和管理包括：

- 设置交换机的名称
- 设置系统时钟
- 时区设置
- 夏令时设置

4.1.1　设置交换机的名称

请在系统视图下进行下列操作。

表4-1　设置交换机的名称

操作	命令
设置交换机的名称	**sysname** *sysname*
恢复交换机名称的缺省值	**undo sysname**

4.1.2　设置系统时钟

请在用户视图下进行下列操作。

表4-2　设置系统时钟

操作	命令
设置系统时钟	**clock datetime** *HH:MM:SS YYYY/MM/DD*

4.1.3　设置时区

该配置任务用于配置本地时区的名称以及相对标准 UTC 时区的时间差。

请在用户视图下进行下列配置。

表4-3 时区设置

操作	命令
设置本地时区	**clock timezone** *zone-name* { **add** | **minus** } *HH:MM:SS*
恢复为缺省的 UTC 时区	**undo clock timezone**

缺省为 UTC 时区。

4.1.4 设置夏令时

该配置任务用于设置夏令时的名称和起始、终止时间。

请在用户视图下进行下列配置。

表4-4 夏令时设置

操作	命令
设置夏令时的名称和时间范围	**clock summer-time** *zone_name* { **one-off** | **repeating** } *start-time start-date end-time end-date offset-time*
取消夏令时设置	**undo clock summer-time**

缺省为无夏令时设置。

4.2 查看系统状态和系统信息

查看系统状态和系统信息的命令根据功能可以划分为以下几类：

- 显示系统配置信息的命令
- 显示系统运行状态的命令
- 显示系统统计信息的命令

有关各协议和各种端口的 display 命令请参见相关章节。下面介绍的 display 命令都用于显示系统的状态和统计信息。

下列操作可以在所有视图下执行。

表4-5 系统 display 命令

操作	命令
显示系统时钟	**display clock**
显示系统版本	**display version**
显示终端用户	**display users** [**all**]

显示起始配置	**display saved-configuration**
显示当前配置	**display current-configuration** [**controller** | **interface** *interface-type* [*interface-number*] | **configuration** [**system** | **user-interface**]] [| { **begin** | **exclude** | **include** } *regular-expression*]
显示调试开关状态	**display debugging** [**interface** { *interface-name* **|** *interface-type interface-number* }] [*moduname*]

4.3 系统调试

4.3.1 打开/关闭调试开关

以太网交换机提供了种类丰富的调试功能，对于以太网交换机所支持的绝大部分协议和功能，系统都提供了相应的调试功能，可以帮助用户对错误进行诊断和定位。

调试信息的输出可以由两个开关控制：

- 协议调试开关，控制是否输出某协议的调试信息。
- 屏幕输出开关，控制是否在某个用户屏幕上输出调试信息。

二者关系如下图所示。

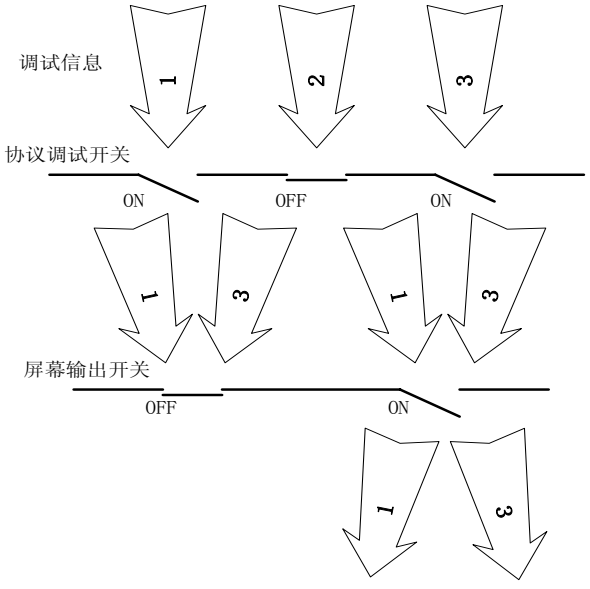


图4-1 调试信息输出示意图

可以使用下面的命令来操作上述两种开关。

请在用户视图下进行下列操作。

表4-6 调试开关的打开和关闭

操作	命令
打开协议调试开关	**debugging** { **all** | *moduname* [*debugging-option*] }
关闭协议调试开关	**undo debugging** { **all** | { *protocol-name* | *function-name* } [*debugging-option*] }
打开屏幕输出开关	**terminal debugging**
关闭屏幕输出开关	**undo terminal debugging**

具体调试命令的使用和调试信息的格式介绍参见相关章节。

📖 说明：

由于调试信息的输出会影响系统的运行效率，请勿轻易打开调试开关，尤其慎用 debugging all 命令，在调试结束后，应关闭全部调试开关。

4.3.2 显示技术支持信息

在以太网交换机出现故障时，可能需要查看很多运行信息来帮助定位问题。各个功能模块都有其对应的运行信息显示命令。这条命令的功能是显示既定的相关模块的运行信息，以供定位分析。

用户可以在所有视图下进行下列操作。

表4-7 显示技术支持信息

操作	命令
显示技术支持信息	**display diagnostic-information**

📖 说明：

用户在使用 **display diagnostic-information** 命令捕获以太网交换机的运行信息时，应该至少连续使用两次，以便比较运行信息的前后差异，以利于故障定位。

4.4 网络连通测试功能

1. ping

可以使用 ping 命令检查网络连接及主机是否可达。ping 命令可以在所有视图下使用。

请在用户视图下进行下列操作。

表4-8 ping 命令

操作	命令
支持 IP 协议 ping	**ping** [-**a** *ip-address*] [**-c** *count*] [**-d**] [-**h** *ttl*] [-**i** {*interface-type interface-num* | *interface-name* }] [**ip**] [**-n**] [**-** **p** *pattern*] [**-q**] [**-r**] [**-s** *packetsize*] [**-t** *timeout*] [**-tos** *tos*] [**-v**] *host*

命令执行结果输出包括：

- 对每一 ping 报文的响应情况，如果超时到仍没有收到响应报文，则输出“Request time out”，否则显示响应报文中数据字节数、报文序号、TTL 和响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

2. tracert

可以使用 tracert 命令测试报文从发送主机到目的地所经过的网关。此命令主要用于检查网络连接是否可达，可以辅助用户分析网络在何处发生了故障。

tracert 的执行过程是：发送主机首先发送一个 TTL 为 1 的数据包，因此第一跳发送回一个 ICMP 错误消息以指明此数据包不能被发送（因为 TTL 超时），之后此数据包被重新发送，TTL 为 2，同样第二跳返回 TTL 超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个 ICMP TTL 超时消息的源地址，以提供一个 IP 数据包到达目的地所经历的路径。

tracert 命令可以在所有视图下使用。

请在用户视图下进行下列操作。

表4-9 tracert 命令

操作	命令
Trace Route	**tracert** [**-a** *source-IP*] [-**f** *first-TTL*] [-**m** *max-TTL*] [-**p** *port*] [-**q** *nqueries*] [-**w** *timeout*] *string*

4.5 信息中心功能

4.5.1 信息中心介绍

信息中心系统是以太网交换机中不可或缺的一部分，它是系统软件模块的信息枢纽。信息中心管理大多数的信息输出，并且能够进行细致的分类，从而能够有效地进行信息筛选。通过与 debugging 程序的结合，信息中心为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

信息格式如下：

<优先级>时间戳 主机名 模块名/级别/信息摘要:内容

```
<priority>timestamp sysname module/level/digest:content
```

以上格式中的尖括号（< >）、空格、斜杠（/）、冒号（:）是有效的、必须的。

输出到日志主机的日志格式的例子如下：

```
<189>Jun 7 05:22:03 2003 Quidway IFNET/6/UPDOWN:Line protocol on
interface Ethernet0/0/0, changed state to UP
```

以下对每一个字段做详细说明。

1. 优先级

优先级的计算按如下公式：facility*8+severity-1，对 VRP 来说，facility 默认为 23，severity 的取值范围为 1～8，含义见对级别的表述。

优先级与时间戳之间没有任何字符。优先级只有信息发送到日志主机上时才能有效。

2. 时间戳

发向日志主机的日志的时间字段是 date 型。

时间戳的格式为“Mmm dd hh:mm:ss yyyy”。

“Mmm”为英语月份的缩写，即为如下的值：Jan，Feb，Mar，Apr，May，Jun，Jul，Aug，Sep，Oct，Nov，Dec。

“dd”为日期，如果日期的值小于 10，则必须写为“空格＋日期”，如“ 7”。

“hh:mm:ss”为本地时间，hh 采用 24 小时制，从 00 到 23；分钟和秒的值均从 00 到 59。

“yyyy”为年份。

时间戳与主机名之间以一个空格隔开。

3. 主机名

主机名是本机的系统名，默认为“Quidway”。

可用 **sysname** 命令修改主机名。

主机名与模块名之间以一个空格隔开。

4. 模块名

该字段表示信息是由哪个模块产生的，部分模块的列表如下：

表4-10 模块名字段列表

模块名	说明
AAA	认证、授权和计费（Authentication，Authorization and Accounting）
ACL	访问控制列表（Access Control List，ACL）
ARP	地址解析协议（Address Resolution Protocol）
ASPF	基于应用层状态的包过滤防火墙（Application Specific Packet Filter）
ATM	异步传输协议（Asynchronous Transfer Mode）
BGP	边界网关协议（Border Gateway Protocol）
CFM	配置文件管理（Configuration File Management）
CHAT	CHAT 验证（PPP 协议使用的一种验证方式）
DCC	拨号控制中心（Dial Control Center）
DHCP	动态主机配置协议（Dynamic Host Configuration Protocol）
ETH	以太网
FILTER	过滤式防火墙
FR	帧中继（Frame Relay）
HDLC	高级数据链路控制（High-level Data Link Control）
HWCM	华为配置管理（HuaWei Configuration Management）
IFNET	接口管理
IKE	因特网密匙交换协议（Internet Key Exchange）
IP	互联网协议（Internet Protocol）
IPHC	IP 头压缩（IP Header Compression）
IPSEC	IP 协议安全扩展 Internet Protocol SECurity extensions
ISIS	中间系统到中间系统（Intermediate System-to-Intermediate System）

模块名	说明
L2TP	二层隧道协议（Layer 2 Tunneling Protocol）
LDP	标签分发协议（Label Distribution Protocol）
LSPAGENT	LSP 代理（Label Switch Path Agent）
LSPM	LSP 管理（Label Switch Path Management）
MODEM	调制解调器
MPLSFW	多协议标记交换转发 Multi-protocol Label Switch Forward
MSDP	组播源发现协议 Multicast Source Discovery Protocol
NAT	网络地址转换（Network Address Translation）
NTP	网络时间协议（Network Time Protocol）
OSPF	开放最短路由优先协议（Open Shortest Path First）
PHY	物理层
POLICY-R	策略路由
PPP	点到点协议（Point to Point Protocol）
PPPOE	以太网承载 PPP 协议（Point-to-Point Protocol over Ethernet）
PPPOE-CL	PPPOE 的 client 端
QoS	服务质量（Quality of Service，简称 QoS）
RM	路由管理（Routing Management）
RSA	RSA 加密系统（Revest，Shamir and Adleman）
RTPRO	路由协议
SHELL	用户界面
SLIP	串行线路 Internet 协议（Serial Line Internet Protocol）
SNMP	简单网络管理协议（Simple Network Management Protocol）
SOCKET	套接字
SSH	安全用户界面（Secure Shell）
STANDBY	备用模块
TELNET	远程登录
TUNNEL	通道
VLAN	虚拟局域网
VOS	虚拟操作系统
VRRP	冗余路由备份协议（Virtual Router Redundancy Protocol）
VTY	虚拟类型终端（Virtual Type Terminal）

模块名与级别之间以一个斜杠(/)隔开。

5. 级别

交换机的信息分为三类：日志信息、调试信息和告警信息。按信息的严重等级或紧急程度，交换机把每类信息都划分为八个等级。在按等级来进行信息过滤时，采用的规则是：禁止严重等级大于所设置阈值的信息输出。越紧急的日志报文，其严重等级越小，emergencies 表示的等级为 0，debugging 为 7，因此，当设置严重等级阈值为 debugging 时，所有的信息都会输出。它们的定义和说明见下表。

表4-11 信息中心定义的优先级（severity）

严重等级	取值	描述
emergencies	1	极其紧急的错误
alerts	2	需立即纠正的错误
critical	3	关键错误
errors	4	需关注但不关键的错误
warnings	5	警告，可能存在某种差错
notifications	6	需注意的信息
informational	7	一般提示信息
debugging	8	调试信息

级别与信息摘要之间以一个斜杠(/)隔开。

6. 信息摘要

信息摘要是一个短语，代表了该信息的内容大意。

信息摘要与内容之间以一个冒号（:）隔开，信息摘要不超过 32 个字符。

4.5.2 信息中心的配置简介

交换机支持信息向 6 个方向进行输出。

目前，系统对每个输出方向缺省分配一个信息通道，请参见下表。

表4-12 输出信息的信息通道名和通道号

输出方向	信息通道号	缺省的信息通道名
控制台	0	console
监视终端	1	monitor
日志主机	2	loghost
告警缓冲区	3	trapbuffer
日志缓冲区	4	logbuffer
snmp	5	snmpagent

📖 **说明：**

六个方向的设置相互独立，但首先需要开启信息中心，其余的设置才会生效。

以太网交换机的信息中心系统具有以下一些特性：

- 支持控制台（ Console ）、监视终端（ monitor ）——Telnet 终端、日志缓冲区（ logbuf ）、日志主机（ loghost ）、告警缓冲区（trapbuf）、SNMP 六个方向的信息输出。
- 信息按重要性划分为八种等级，可按等级进行信息过滤。
- 信息按来源模块进行划分，可按模块进行信息过滤。
- 信息在输出时可以进行中英文选择。

(1) 配置信息发送到日志主机。

表4-13 配置信息发送到日志主机

设备	配置	缺省值	配置说明
Switch	启动信息中心	缺省情况下，信息中心处于开启状态。	只有启动了信息中心，其他配置才能有效。
	配置信息输出方向为 loghost	-	交换机上关于日志主机的配置和日志主机上的配置一定要保持一致，否则信息将无法正确发送到日志主机上。
	配置信息源	—	用户可以定义哪些模块、哪些信息能够发送出去、信息的时间戳格式等。如果用户定义输出调试信息，则需要打开相应模块的调试开关。
日志主机	日志主机的相关配置请参考配置案例。	-	—

(2)　配置信息发送到控制台。

表4-14 配置信息发送到控制台

设备	配置	缺省值	配置说明
Switch	启动信息中心	缺省情况下，信息中心处于开启状态。	只有启动了信息中心，其他配置才能有效。
	配置信息输出方向为 Console	-	-
	配置信息源	—	用户可以定义哪些模块、哪些信息能够发送出去、信息的时间戳格式等。如果用户定义输出调试信息，则需要打开相应模块的调试开关。
	打开终端显示功能	-	打开终端显示功能，用户才能看到调试信息。

(3)　配置信息发送到监视终端。

表4-15 配置信息发送到监控终端

设备	配置	缺省值	配置说明
Switch	启动信息中心	缺省情况下，信息中心处于开启状态。	只有启动了信息中心，其他配置才能有效。
	配置信息输出方向为 monitor	-	-
	配置信息源	—	用户可以定义哪些模块、哪些信息能够发送出去、信息的时间戳格式等。如果用户定义输出调试信息，则需要打开相应模块的调试开关。
	打开当前终端显示功能及相应信息的终端显示功能	-	对于 Telnet 终端和哑终端，必须使用 terminal monitor 命令打开当前终端显示功能，用户才能看到信息。

(4)　配置信息发送到日志缓冲区。

表4-16 配置信息发送到日志缓冲区

设备	配置	缺省值	配置说明
Switch	启动信息中心	缺省情况下，信息中心处于开启状态。	只有启动了信息中心，其他配置才能有效。
	配置信息输出方向为 logbuffer	-	用户可以同时配置交换机日志缓冲区的大小
	配置信息源	—	用户可以定义哪些模块、哪些信息能够发送出去、信息的时间戳格式等。如果用户定义输出调试信息，则需要打开相应模块的调试开关。

(5)　配置信息发送到告警缓冲区。

表4-17 配置信息发送到告警缓冲区

设备	配置	缺省值	配置说明
Switch	启动信息中心	缺省情况下，信息中心处于开启状态。	只有启动了信息中心，其他配置才能有效。
	配置信息输出方向为 trapbuffer	-	用户可以同时配置交换机告警缓冲区的大小
	配置信息源	—	用户可以定义哪些模块、哪些信息能够发送出去、信息的时间戳格式等。如果用户定义输出调试信息，则需要打开相应模块的调试开关。

(6)　配置信息发送到 SNMP。

表4-18 配置信息发送到 SNMP

设备	配置	缺省值	配置说明
Switch	启动信息中心	缺省情况下，信息中心处于开启状态。	只有启动了信息中心，其他配置才能有效。
	配置信息输出方向为 SNMP	-	-
	配置信息源	—	用户可以定义哪些模块、哪些信息能够发送出去、信息的时间戳格式等。如果用户定义输出调试信息，则需要打开相应模块的调试开关。
	SNMP 特性配置	-	请参考 SNMP 章节的描述
网管工作站	和交换机的 SNMP 配置保持一致	-	-

4.5.3 配置信息发送到日志主机

配置信息发送到日志主机需要经过如下配置

(1)　开启信息中心。

请在系统视图下进行下列操作。

表4-19 开启或关闭信息中心

操作	命令
开启信息中心	**info-center enable**
关闭信息中心	**undo info-center enable**

📖 **说明：**

信息中心缺省情况下处于开启状态。信息中心开启时，由于信息分类、输出的原因，在处理信息较多时，对系统性能有一定的影响。

(2)　在交换机上配置向日志主机输出信息。

请在系统视图下进行下列操作。

表4-20 配置向日志主机输出信息

操作	命令
向日志主机输出信息	**info-center loghost** *host-ip-addr* [**channel** { *channel-number* | *channel-name* }] [**facility** *local-number*] [**language** { **chinese** | **english** }]
取消向日志主机输出信息	**undo info-center loghost** *host-ip-addr*

请注意配置正确的日志主机 IP 地址。

📖 **说明：**

使用命令 **info-center loghost** 配置日志主机的 IP 地址时，请输入正确的 IP 地址。如果用户输入的是环回地址，系统将提示此地址无效。

(3)　在交换机上配置信息源。

本配置可以定义发送到日志主机上的信息是哪些模块产生的、信息的类型、信息的级别等。

请在系统视图下进行下列操作。

表4-21 定义信息源

操作	命令
定义信息源	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
删除信息源的配置	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name 是模块名；**default** 代表所有模块；**level** 是信息重要级别；*severity* 是信息级别，在此级别以下的信息不输出；*channel-number* 是要设置的信息通道号；*channel-name* 是要设置的信息通道名。

在定义发送到日志主机上的信息时 *channel-number* 或者 *channel-name* 要设定为 loghost 方向对应的通道。

对每个信息通道设有一条缺省记录，它的模块名为 **default**，模块号为 0xffff0000，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，系统使用这条缺省的配置记录。

📖 **说明：**

当用户需要查看交换机某些模块的调试信息时，需要在配置信息源时将信息类别选择为 **debugging**，同时使用 **debugging** 命令开启相应模块的调试开关。

用户可以使用下面的命令来配置日志信息、调试信息和告警信息的时间戳输出格式。此配置将影响到用户看到的信息的时间戳格式。

请在系统视图下进行下列操作。

表4-22 配置时间戳输出格式

操作	命令
配置时间戳输出格式	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
禁止输出时间戳字段	**undo info-center timestamp** { **log** | **trap** | **debugging** }

(4)　日志主机的配置。

日志主机上的配置要和交换机上对日志主机的配置保持一致。日志主机的相关配置可以参考后面的配置举例。

4.5.4 配置信息发送到控制台

配置信息发送到控制台需要经过如下配置。

(1)　开启信息中心。

请在系统视图下进行下列操作。

表4-23 开启或关闭信息中心

操作	命令
开启信息中心	**info-center enable**
关闭信息中心	**undo info-center enable**

📖 **说明：**

信息中心缺省情况下处于开启状态。信息中心开启时，由于信息分类、输出的原因，在处理信息较多时，对系统性能有一定的影响。

(2)　在交换机上配置向控制台输出信息。

请在系统视图下进行下列操作。

表4-24 配置向控制台输出信息

操作	命令
向 Console 方向输出信息	**info-center console channel**{ *channel-number* | *channel-name* }
取消向 Console 方向输出信息	**undo info-center console channel**

(3)　在交换机上配置信息源。

本配置可以定义发送到控制台上的信息是哪些模块产生的、信息的类型、信息的级别等。

请在系统视图下进行下列操作。

表4-25 定义信息源

操作	命令
定义信息源	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
删除信息源的配置	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name 是模块名；**default** 代表所有模块；**level** 是信息重要级别；*severity* 是信息级别，在此级别以下的信息不输出；*channel-number* 是要设置的信息通道号；*channel-name* 是要设置的信息通道名。

在定义发送到控制台上的信息时 *channel-number* 或者 *channel-name* 要设定为 Console 方向对应的通道。

对每个信息通道设有一条缺省记录，它的模块名为 **default**，模块号为 0xffff0000，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，系统使用这条缺省的配置记录。

📖 **说明：**

当用户需要查看交换机某些模块的调试信息时，需要在配置信息源时将信息类别选择为 **debugging**，同时使用 **debugging** 命令开启相应模块的调试开关。

用户可以使用下面的命令来配置日志信息、调试信息和告警信息的时间戳输出格式。此配置将影响到用户看到的信息的时间戳格式。

请在系统视图下进行下列操作。

表4-26 配置时间戳输出格式

操作	命令
配置时间戳输出格式	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
禁止输出时间戳字段	**undo info-center timestamp** { **log** | **trap** | **debugging** }

(4)　打开终端显示功能。

对于交换机发往控制台的日志、调试和告警信息，用户需要首先在交换机上打开相应的日志、调试和告警显示功能，才能从控制台上观察到输出的信息。

例如，如果用户在配置了发往控制台的信息为日志信息后，需要在交换机上使用命令 **terminal logging** 打开终端显示日志信息功能，这样用户才可能从控制台上观察到交换机发送过来的日志信息。

请在用户视图下进行下列操作。

表4-27 打开终端显示功能

操作	命令
打开终端显示调试信息功能	**terminal debugging**
关闭终端显示调试信息功能	**undo terminal debugging**
打开终端显示日志信息功能	**terminal logging**
关闭终端显示日志信息功能	**undo terminal logging**
打开终端告警信息显示功能	**terminal trapping**
关闭终端显示告警信息功能	**undo terminal trapping**

4.5.5 配置信息发送到 Telnet 终端或哑终端

配置信息发送到 Telnet 终端或哑终端需要经过如下配置

(1)　开启信息中心。

请在系统视图下进行下列操作。

表4-28 开启或关闭信息中心

操作	命令
开启信息中心	**info-center enable**
关闭信息中心	**undo info-center enable**

📖 **说明：**

信息中心缺省情况下处于开启状态。信息中心开启时，由于信息分类、输出的原因，在处理信息较多时，对系统性能有一定的影响。

(2)　在交换机上配置向 Telnet 终端或哑终端输出信息。

请在系统视图下进行下列操作。

表4-29 配置向 Telnet 终端或哑终端输出信息

操作	命令
向 Telnet 终端或哑终端输出信息	**info-center monitor channel** { *channel-number* | *channel-name* }
取消向 Telnet 终端或哑终端输出信息	**undo info-center monitor channel**

(3)　在交换机上配置信息源。

本配置可以定义发送到 Telnet 终端或哑终端的信息是哪些模块产生的、信息的类型、信息的级别等。

请在系统视图下进行下列操作。

表4-30 定义信息源

操作	命令
定义信息源	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
删除信息源的配置	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name 是模块名；**default** 代表所有模块；**level** 是信息重要级别；*severity* 是信息级别，在此级别以下的信息不输出；*channel-number* 是要设置的信息通道号；*channel-name* 是要设置的信息通道名。

在定义发送到 Telnet 终端或哑终端的信息时 *channel-number* 或者 *channel-name* 要设定为 monitor 方向对应的通道。

对每个信息通道设有一条缺省记录，它的模块名为 **default**，模块号为 0xffff0000，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，系统使用这条缺省的配置记录。

🕮 **说明：**

同时有多个 Telnet 用户或哑终端用户时，各个用户之间共享一些配置参数，其中包括按模块过滤设置，中英文选择，严重等级阈值，某一个用户改变这些设置时，在别的用户端也有所反映。

🕮 **说明：**

当用户需要查看交换机某些模块的调试信息时，需要在配置信息源时将信息类别选择为 **debugging**，同时使用 **debugging** 命令开启相应模块的调试开关。

用户可以使用下面的命令来配置日志信息、调试信息和告警信息的时间戳输出格式。此配置将影响到用户看到的信息的时间戳格式。

请在系统视图下进行下列操作。

表4-31 配置时间戳输出格式

操作	命令
配置时间戳输出格式	**info-center timestamp { log | trap | debugging } { boot | date | none }**
禁止输出时间戳字段	**undo info-center timestamp { log | trap | debugging }**

(4)　打开终端显示功能。

对于交换机发往 Telnet 终端或哑终端的日志、调试和告警信息，用户需要首先在交换机上打开当前终端显示功能，然后打开相应的终端信息显示功能，才能从 Telnet 终端或哑终端上观察到输出的信息。

例如，如果用户在配置了发往控制台的信息为日志信息后，需要在交换机上使用命令 **terminal monitor** 打开当前终端显示功能，然后使用命令 **terminal logging** 打开终端日志信息功能，这样用户才可能从 Telnet 终端或哑终端上观察到交换机发送过来的日志信息。

请在用户视图下进行下列操作。

表4-32 打开终端显示功能

操作	命令
打开终端信息显示系统日志发送的调试/日志/告警信息功能	**terminal monitor**
关闭终端显示上述信息功能	**undo terminal monitor**
打开终端显示调试信息功能	**terminal debugging**
关闭终端显示调试信息功能	**undo terminal debugging**
打开终端显示日志信息功能	**terminal logging**
关闭终端显示日志信息功能	**undo terminal logging**
打开终端告警信息显示功能	**terminal trapping**
关闭终端显示告警信息功能	**undo terminal trapping**

4.5.6 配置信息发送到日志缓冲区

配置信息发送到日志缓冲区需要经过如下配置。

(1)　开启信息中心。

请在系统视图下进行下列操作。

表4-33 开启或关闭信息中心

操作	命令
开启信息中心	**info-center enable**
关闭信息中心	**undo info-center enable**

📖 **说明：**

信息中心缺省情况下处于开启状态。信息中心开启时，由于信息分类、输出的原因，在处理信息较多时，对系统性能有一定的影响。

(2)　在交换机上配置向日志缓冲区输出信息。

请在系统视图下进行下列操作。

表4-34 配置向日志缓冲区输出信息

操作	命令
向日志缓冲区输出信息	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* }] [**size** *buffersize*]
取消向日志缓冲区输出信息	**undo info-center logbuffer** [**channel** | **size**]

(3)　在交换机上配置信息源。

本配置可以定义发送到日志缓冲区的信息是哪些模块产生的、信息的类型、信息的级别等。

请在系统视图下进行下列操作。

表4-35 定义信息源

操作	命令
定义信息源	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
删除信息源的配置	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name 是模块名；**default** 代表所有模块；**level** 是信息重要级别；*severity* 是信息级别，在此级别以下的信息不输出；*channel-number* 是要设置的信息通道号；*channel-name* 是要设置的信息通道名。

在定义发送到日志缓冲区的信息时 *channel-number* 或者 *channel-name* 要设定为 logbuffer 方向对应的通道。

对每个信息通道设有一条缺省记录，它的模块名为 **default**，模块号为 0xffff0000，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，系统使用这条缺省的配置记录。

📖 **说明：**

当用户需要查看交换机某些模块的调试信息时，需要在配置信息源时将信息类别选择为 **debugging**，同时使用 **debugging** 命令开启相应模块的调试开关。

用户可以使用下面的命令来配置日志信息、调试信息和告警信息的时间戳输出格式。此配置将影响到用户看到的信息的时间戳格式。

请在系统视图下进行下列操作。

表4-36 配置时间戳输出格式

操作	命令
配置时间戳输出格式	**info-center timestamp { log | trap | debugging } { boot | date | none }**
禁止输出时间戳字段	**undo info-center timestamp { log | trap | debugging }**

4.5.7 配置信息发送到告警缓冲区

配置信息发送到告警缓冲区需要经过如下配置。

(1) 开启信息中心。

请在系统视图下进行下列操作。

表4-37 开启或关闭信息中心

操作	命令
开启信息中心	**info-center enable**
关闭信息中心	**undo info-center enable**

📖 **说明：**

信息中心缺省情况下处于开启状态。信息中心开启时，由于信息分类、输出的原因，在处理信息较多时，对系统性能有一定的影响。

(2)　在交换机上配置向告警缓冲区输出信息。

请在系统视图下进行下列操作。

表4-38 配置向告警缓冲区输出信息

操作	命令
向告警缓冲区输出信息	**info-center trapbuffer** [**size** *buffersize*] [**channel** { *channel-number* | *channel-name* }]
取消向告警缓冲区输出信息	**undo info-center trapbuffer** [**channel** | **size**]

(3)　在交换机上配置信息源。

本配置可以定义发送到告警缓冲区的信息是哪些模块产生的、信息的类型、信息的级别等。

请在系统视图下进行下列操作。

表4-39 定义信息源

操作	命令
定义信息源	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
删除信息源的配置	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name 是模块名；**default** 代表所有模块；**level** 是信息重要级别；*severity* 是信息级别，在此级别以下的信息不输出；*channel-number* 是要设置的信息通道号；*channel-name* 是要设置的信息通道名。

在定义发送到告警缓冲区的信息时 *channel-number* 或者 *channel-name* 要设定为 trapbuffer 方向对应的通道。

对每个信息通道设有一条缺省记录，它的模块名为 **default**，模块号为 0xffff0000，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，系统使用这条缺省的配置记录。

🕮 **说明：**

当用户需要查看交换机某些模块的调试信息时，需要在配置信息源时将信息类别选择为 **debugging**，同时使用 **debugging** 命令开启相应模块的调试开关。

用户可以使用下面的命令来配置日志信息、调试信息和告警信息的时间戳输出格式。此配置将影响到用户看到的信息的时间戳格式。

请在系统视图下进行下列操作。

表4-40 配置时间戳输出格式

操作	命令
配置时间戳输出格式	**info-center timestamp { log | trap | debugging } { boot | date | none }**
禁止输出时间戳字段	**undo info-center timestamp { log | trap | debugging }**

4.5.8 配置信息发送到 SNMP 网管

配置信息发送到 SNMP 网管需要经过如下配置。

(1)　开启信息中心。

请在系统视图下进行下列操作。

表4-41 开启或关闭信息中心

操作	命令
开启信息中心	**info-center enable**
关闭信息中心	**undo info-center enable**

🕮 **说明：**

信息中心缺省情况下处于开启状态。信息中心开启时，由于信息分类、输出的原因，在处理信息较多时，对系统性能有一定的影响。

(2)　在交换机上配置向 SNMP 网管输出信息。

请在系统视图下进行下列操作。

表4-42 配置向 SNMP 网管输出信息

操作	命令
向 SNMP 输出信息	**info-center snmp channel** { *channel-number* | *channel-name* }
取消向 SNMP 输出信息	**undo info-center snmp channel**

(3)　在交换机上配置信息源。

本配置可以定义发送到 SNMP 的信息是哪些模块产生的、信息的类型、信息的级别等。

请在系统视图下进行下列操作。

表4-43 定义信息源

操作	命令
定义信息源	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
删除信息源的配置	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name 是模块名；**default** 代表所有模块；**level** 是信息重要级别；*severity* 是信息级别，在此级别以下的信息不输出；*channel-number* 是要设置的信息通道号；*channel-name* 是要设置的信息通道名。

在定义发送到 SNMP 网管上的信息时 *channel-number* 或者 *channel-name* 要设定为 SNMP 方向对应的通道。

对每个信息通道设有一条缺省记录，它的模块名为 **default**，模块号为 0xffff0000，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，系统使用这条缺省的配置记录。

📖 **说明：**

当用户需要查看交换机某些模块的调试信息时，需要在配置信息源时将信息类别选择为 **debugging**，同时使用 **debugging** 命令开启相应模块的调试开关。

用户可以使用下面的命令来配置日志信息、调试信息和告警信息的时间戳输出格式。此配置将影响到用户看到的信息的时间戳格式。

请在系统视图下进行下列操作。

表4-44 配置时间戳输出格式

操作	命令
配置时间戳输出格式	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
禁止输出时间戳字段	**undo info-center timestamp** { **log** | **trap** | **debugging** }

(4)　交换机上 SNMP 的配置和网管工作站的配置。

为了使信息可以正确发送到SNMP网管，交换机上还需要对SNMP进行配置，同时在远端的网管工作站上也需要作相应的配置。这样才能在网管工作站上获得正确的信息。SNMP可以参见后续的 第 5 章　SNMP配置。

4.5.9 信息中心的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后信息中心的运行情况。用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **reset** 命令可以将信息中心统计信息清除。

请在用户视图下进行下列操作。**display** 命令还可以在所有视图下进行。

表4-45 信息中心显示和调试

操作	命令
显示信息通道的内容	**display channel** [*channel-number* | *channel-name*]
显示系统日志的配置及内存缓冲区记录的信息	**display info-center**
清除日志缓冲区内的信息	**reset logbuffer**
清除告警缓冲区内的信息	**reset trapbuffer**

4.5.10 日志发送到 UNIX 日志主机的配置举例

1. 组网需求

交换机的日志信息发送到 Unix 日志主机上，日志主机的 IP 地址为 202.38.1.10，严重等级高于 informational 的日志信息将会发送到日志主机上，输出语言为英文，允许输出信息的模块为 ARP 和 IP

2. 组网图

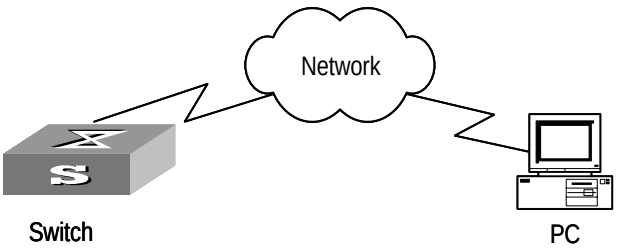


图4-2 配置示意图

3. 配置步骤

(1)　交换机上的配置。

开启信息中心。

[Quidway] info-center enable

将 IP 地址为 202.38.1.10 的主机用作日志主机，设置严重等级阈值为 informational，输出语言为英文，允许输出信息的模块为 ARP 和 IP。

[Quidway] info-center loghost 202.38.1.10 facility local4 language english

[Quidway] info-center source arp channel loghost log level informational

[Quidway] info-center source ip channel loghost log level informational

(2)　日志主机上的配置。

此配置是在日志主机上进行的配置。下面的配置示例是在 SunOS 4.0 上完成的，在其它厂商的 Unix 操作系统上的配置操作基本与之相同。

第一步：以超级用户（root）的身份执行以下命令。

mkdir /var/log/Quidway

touch /var/log/Quidway/information

第二步：以超级用户（root）的身份编辑文件/etc/syslog.conf，加入以下选择/动作组合（selector/action pairs）。

Quidway configuration messages

local4.info　/var/log/Quidway/information

📖 说明：

在编辑/etc/syslog.conf 时应注意以下问题:
(1) 注释只允许独立成行，并以字符# 开头。
(2) 选择/动作组合之间必须以一个制表符分隔，而不能输入空格。
(3) 在文件名之后不得有多余的空格。
(4) /etc/syslog.conf 中指定的设备名及接受的日志信息级别与交换机上配置的 info-center loghost 和 info-center loghost a.b.c.d facility 应保持一致，否则日志信息可能无法正确输出到日志主机上。

第三步：当日志文件 information 建立且/etc/syslog.conf 文件被修改了之后，应通过执行以下命令给系统守护进程 syslogd 一个 HUP 信号来使 syslogd 重新读取它的配置文件/etc/syslog.conf。

ps -ae | grep syslogd

147

kill -HUP 147

进行以上操作之后，交换机系统就可以在相应的日志文件中记录信息了。

📖 说明：

综合配置设备名称（facility）、严重等级阈值（severity）、模块名称（filter）以及 syslog.conf 文件，可以进行相当细致的分类，达到信息筛选的目的。

4.5.11 日志发送到 LINUX 日志主机的配置举例

1. 组网需求

交换机的日志信息发送到 Linux 日志主机上，日志主机的 IP 地址为 202.38.1.10，严重等级高于 informational 的日志信息将会发送到日志主机上，输出语言为英文，允许输出信息的模块为所有模块。

2. 组网图

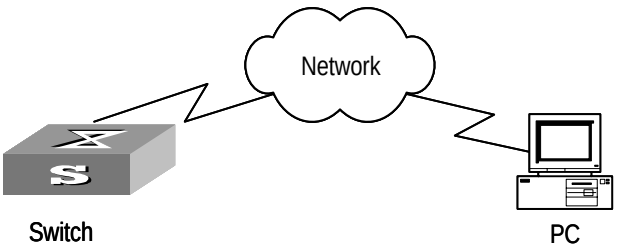


图4-3 配置示意图

3. 配置步骤

(1)　交换机上的配置。

开启信息中心。

[Quidway] info-center enable

将 IP 地址为 202.38.1.10 的主机用作日志主机，设置严重等级阈值为 informational，输出语言为英文，允许输出信息的模块为所有模块。

[Quidway] info-center loghost 202.38.1.10 facility local7 language english

[Quidway] info-center source default channel loghost log level informational

(2)　日志主机上的配置。

此配置是在日志主机上进行的配置。

第一步：以超级用户（root）的身份执行以下命令。

mkdir /var/log/Quidway

touch /var/log/Quidway/information

第二步：以超级用户（root）的身份编辑文件/etc/syslog.conf，加入以下选择/动作组合（selector/action pairs）。

Quidway configuration messages

local7.info　/var/log/Quidway/information

📖 说明：

在编辑/etc/syslog.conf 时应注意以下问题:
(1) 注释只允许独立成行，并以字符# 开头。
(2) 选择/动作组合之间必须以一个制表符分隔，而不能输入空格。
(3) 在文件名之后不得有多余的空格。
(4) /etc/syslog.conf 中指定的设备名及接受的日志信息级别与交换机上配置的 info-center loghost 和 info-center loghost a.b.c.d facility 应保持一致，否则日志信息可能无法正确输出到日志主机上。

第三步：当日志文件 information 建立且/etc/syslog.conf 文件被修改了之后，应通过执行以下命令查看系统守护进程 syslogd 的进程号，杀死 syslogd 进程，并重新用-r 选项在后台启动 syslogd。

```
# ps -ae | grep syslogd

147

# kill -9 147

# syslogd -r &
```

📖 说明：

对 Linux 日志主机，必须保证 syslogd 进程是以-r 选项启动。

进行以上操作之后，交换机系统就可以在相应的日志文件中记录信息了。

📖 说明：

综合配置设备名称（facility）、严重等级阈值（severity）、模块名称（filter）以及 syslog.conf 文件，可以进行相当细致的分类，达到信息筛选的目的。

4.5.12 日志发送到控制台的配置举例

1. 组网需求

交换机的日志信息发送到控制台上，严重等级高于 informational 的日志信息将会发送到日志主机上，输出语言为英文，允许输出信息的模块为 ARP 和 IP

2. 组网图

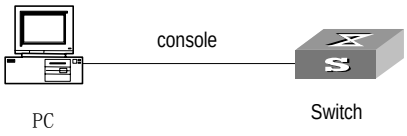


图4-4 配置示意图

3. 配置步骤

(1)　交换机上的配置

开启信息中心。

[Quidway] info-center enable

配置控制台日志输出，允许 ARP 和 IP 模块的日志输出，严重等级限制为 emergencies～informational。

[Quidway] info-center console channel console

[Quidway] info-center source arp channel console log level informational

[Quidway] info-center source ip channel console log level informational

打开终端显示功能。

<Quidway> terminal logging

第5章 SNMP 配置

5.1 SNMP 协议介绍

目前网络中用得最广泛的网络管理协议是 SNMP（Simple Network Management Protocol）。SNMP 是被广泛接受并投入使用的工业标准，用于保证管理信息在任意两点间传送，便于网络管理员在网络上的任何节点检索信息、修改信息、寻找故障、完成故障诊断、进行容量规划和生成报告。SNMP 采用轮询机制，只提供最基本的功能集，特别适合在小型、快速和低价格的环境中使用。SNMP 的实现基于连接的传输层协议 UDP，得到众多产品的支持。

SNMP 分为 NMS 和 Agent 两部分，NMS（Network Management Station），是运行客户端程序的工作站，目前常用的网管平台有 Sun NetManager 和 IBM NetView；Agent 是运行在网络设备上的服务器端软件。NMS 可以向 Agent 发出 GetRequest、GetNextRequest 和 SetRequest 报文，Agent 接收到 NMS 的请求报文后，根据报文类型进行 Read 或 Write 操作，生成 Response 报文，并将报文返回给 NMS。Agent 在设备发现重新启动等异常情况时，也会主动向 NMS 发送 Trap 报文，向 NMS 汇报所发生的事件。

5.2 SNMP 版本及支持的 MIB

为了在 SNMP 报文中唯一标识设备中的管理变量，SNMP 用层次结构命名方案来识别管理对象。用层次结构命名的管理对象的集合就象一棵树，树的节点表示管理对象，如下图所示。管理对象可以用从根开始的一条路径别无二义地识别。

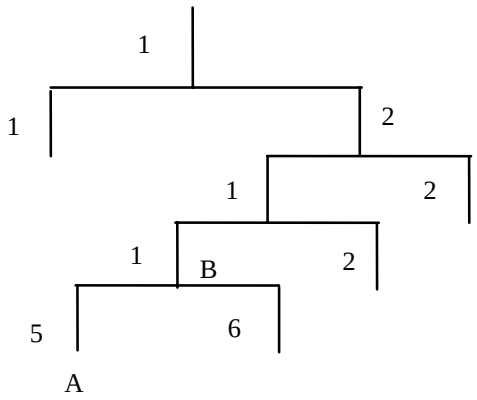


图5-1 MIB 树结构

MIB（Management Information Base）的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。在上图中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的 Object Identifier（客体标识符）。

以太网交换机中的 SNMP Agent 支持 SNMP V1、V2C 和 V3，支持的常见 MIB 如下表所示。

表5-1 以太网交换机支持的常见 MIB

MIB 属性	MIB 内容	参见资料
公有 MIB	基于 TCP/IP 网络设备的 MIB II	参见 RFC1213
	BRIDGE MIB	参见 RFC1493
		参见 RFC2675
	RIP MIB	参见 RFC1724
	RMON MIB	参见 RFC2819
	以太网 MIB	参见 RFC2665
	OSPF MIB	参见 RFC1253
	IF MIB	参见 RFC1573
私有 MIB	DHCP MIB	
	QACL MIB	
	ADBM MIB	
	RSTP MIB	
	VLAN MIB	
	设备管理	
	接口管理	

5.3 配置 SNMP

SNMP 的主要配置包括：

- 设置团体名
- 设置 sysContact
- 允许或禁止发送 Trap
- 设置 Trap 目标主机的地址
- 设置 sysLocation
- 配置本地或远端设备的名字
- 配置一个 SNMP 的组
- 指定发送 Trap 的源地址
- 为一个 SNMP 的组添加一个新用户
- 创建或者更新视图的信息
- 设置 Agent 能接收/发送的 SNMP 消息包的大小

5.3.1 设置团体名

SNMPV1、SNMPV2C 采用团体名认证。SNMP 团体（Community）用一个字符串来命名，称为团体名（Community Name）。SNMP 团体名用来定义 SNMP manager 和 SNMP agent 的关系。团体名起到了类似于密码的作用，可以限制 SNMP manager 访问以太网交换机上的 SNMP agent。用户可以选择指定以下一个或者多个与团体名相关的特性：

- 定义团体（community）可以访问的所有 MIB 对象的子集的 MIB 视图；
- 团体可以访问的 MIB 对象的读写（read-write）或者只读（read-only）权限。具有只读权限的团体只能对设备信息进行查询，而具有读写权限的团体还可以对设备进行配置。

请在系统视图下进行下列配置。

表5-2 设置团体名

操作	命令
设置团体名及访问权限	**snmp-agent community** { **read** | **write** } *community-name* [[**mib-view** *view-name*] [**acl** *acl-list*]]
取消团体名及访问权限	**undo snmp-agent community** *community-name*

5.3.2 设置管理员的标识及联系方法

sysContact 是描述系统维护联系信息的字符串，设备维护人员可以利用维护信息了解该设备的生产厂商等信息，如果设备发生故障，设备维护人员可以利用系统维护联系信息，及时与设备生产厂商取得联系。可以使用下面的命令来设置系统维护联系信息。

请在系统视图下进行下列配置。

表5-3 设置管理员的标识及联系方法

操作	命令
设置管理员的标识及联系方法	**snmp-agent sys-info contact** *sysContact*
恢复管理员的标识及联系方法为缺省值	**undo snmp-agent sys-info contact**

5.3.3 设置以太网交换机的位置信息

sysLocation 是 MIB 中 system 组的一个管理变量，用于表示被管理设备的位置。

可以使用下面的命令来设置以太网交换机的位置信息。

请在系统视图下进行下列配置。

表5-4 设置以太网交换机的位置信息

操作	命令
设置以太网交换机的位置信息	**snmp-agent sys-info location** *sysLocation*
恢复以太网交换机的位置信息的缺省设置	**undo snmp-agent sys-info location**

缺省情况下 *sysLocation* 为“Beijing China”。

5.3.4 设置 SNMP 的版本信息

可以使用下面的命令来设置以太网交换机的 SNMP 的版本信息。

请在系统视图下进行下列配置。

表5-5 设置 SNMP 的版本信息

操作	命令
设置 SNMP 的版本信息	**snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }
恢复 SNMP 的版本信息的缺省设置	**undo snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }

5.3.5 允许或禁止发送 Trap

Trap 是被管理设备主动向 NMS 发送的不经请求的信息，用于报告一些紧急的重要事件（如被管理设备重新启动等）。

可以使用下面的命令来允许或禁止被管理设备发送 Trap 信息。

请在系统视图下进行下列配置。

表5-6 允许或禁止发送 Trap

操作	命令
允许发送 Trap	**snmp-agent trap enable** [**standard** [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]
禁止发送 Trap	**undo snmp-agent trap enable** [**standard** [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]

5.3.6 设置 Trap 目标主机的地址

可以使用下面的命令来设置或删除发送 Trap 信息的目标主机的 IP 地址。

请在系统视图下进行下列配置。

表5-7 设置 Trap 目标主机的地址

操作	命令
设置 Trap 目标主机地址	**snmp-agent target-host trap address udp-domain** *host-addr* [**udp-port** *udp-port-number*] **params securityname** *community-string* [**v1 | v2c | v3** { **authentication | privacy** }]
删除 Trap 目标主机地址	**undo snmp-agent target-host** *host-addr* **securityname** *community-string*

5.3.7 设置 Trap 报文的保存时间

可以适用下面的命令用来设置 Trap 报文的保存时间，超过该时间的 Trap 报文都将被丢弃。

请在系统视图下进行下列配置。

表5-8 设置 Trap 报文的保存时间

操作	命令
设置 Trap 报文的保存时间	**snmp-agent trap life** *seconds*
恢复 Trap 报文保存时间的缺省值	**undo snmp-agent trap life**

缺省的 Trap 报文保存时间为 120 秒。

5.3.8 设置本地或远端设备的引擎 ID

可以使用下面的命令来设置本地或远端设备的引擎 ID。

请在系统视图下进行下列配置。

表5-9 设置本地或远端设备的引擎 ID

操作	命令
设置设备的引擎 ID	**snmp-agent local-engineid** *engineid*
设置设备的引擎 ID 为缺省值	**undo snmp-agent local-engineid**

设备引擎 ID 必须是 16 进制数字，至少 5 个字符，可以是 IP 地址、MAC 地址或自己定义的文本，缺省为公司的企业号+设备信息。

5.3.9 设置或删除一个 SNMP 的组

可以使用下面的命令来设置或删除 SNMP 的一个组

请在系统视图下进行下列配置。

表5-10 设置或删除一个 SNMP 组

操作	命令
设置一个 SNMP 组	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*]
删除一个 SNMP 组	**undo snmp-agent group** { **v1 | v2c** } **undo snmp-agent group v3** *group-name* [**authentication | privacy**]

5.3.10 指定发送 Trap 的源地址

可以使用下面的命令来设定或取消发送 Trap 的源地址。

请在系统视图下进行下列配置。

表5-11 设定发送 Trap 的源地址

操作	命令
指定发送 Trap 的源地址	**snmp-agent trap source** *interface-name interface-num*
取消发送 Trap 的源地址	**undo snmp-agent trap source**

5.3.11 SNMP 组添加一个新用户或删除一个用户

可以使用下面的命令来为 SNMP 组添加或删除一个用户。

请在系统视图下进行下列配置。

表5-12 SNMP 组添加或删除一个用户

操作	命令
为 SNMP 组添加一个新用户	**snmp-agent usm-user** { **v1 | v2c** } *username groupname* [**acl** *acl-list*] **snmp-agent usm-user v3** *username groupname* [**authentication-mode** { **md5** | **sha** } *authpassstring* [**privacy-mode** { **des56** *privpassstring* }]] [**acl** *acl-list*]
删除 SNMP 组的一个用户	**undo snmp-agent usm-user** { **v1** | **v2c** } *username groupname* **undo snmp-agent usm-user v3** *username groupname* ｛ **local** | **engineid** *engine-id* }

5.3.12 创建或更新视图的信息或删除视图

用户可以为团体指定视图，以限制 SNMP manager 可以访问的 MIB 对象。用户可以使用预先定义的视图，也可以自己生成视图。可以使用下面的命令创建、更新视图的信息或删除视图。

请在系统视图下进行下列配置。

表5-13 创建、更新视图的信息或删除视图

操作	命令
创建或更新视图的信息	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree*
删除视图	**undo snmp-agent mib-view** *view-name*

5.3.13 设置 Agent 接收/发送的 SNMP 消息包的大小

可以使用下面的命令来设置 Agent 能接收/发送的 SNMP 消息包的大小。

请在系统视图下进行下列配置。

表5-14 设置 Agent 能接收/发送的 SNMP 消息包的大小

操作	命令
设置 Agent 能接收/发送的 SNMP 消息包的大小	**snmp-agent packet max-size** *byte-count*
恢复 SNMP 消息包的大小的缺省值	**undo snmp-agent packet max-size**

Agent 能接收/发送的 SNMP 消息包大小的取值范围为 484～17940，单位为字节，缺省值为 1500 字节。

5.3.14 禁止 SNMP Agent 运行

要禁止 SNMP Agent 的运行，请在系统视图下进行如下配置。

表5-15 禁止 SNMP Agent 运行

操作	命令
禁止 SNMP Agent 运行	**undo snmp-agent**

禁止 SNMP Agent 运行以后，用户配置任何一条 **snmp-agent** 命令，都将重新启动 SNMP Agent。

5.4 SNMP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 SNMP 的运行情况，通过查看显示信息验证配置的效果。

表5-16 SNMP 的显示和调试

操作	命令
显示 SNMP 报文统计信息	**display snmp-agent statisitics**
显示当前设备的引擎 ID	**display snmp-agent** { **local-engineid** | **remote-engineid** }
显示交换机上的组名、安全模式、各种视图的状态以及各组存储方式	**display snmp-agent group** [*group-name*]
显示组用户名表中的 SNMP 用户信息	**display snmp-agent usm-user** [**engineid** *engineid*] [**group** *groupname*] [**username** *username*]
显示当前配置的团体名	**display snmp-agent community** [**read** | **write**]
显示当前配置的 MIB 视图	**display snmp-agent mib-view** [**exclude** | **include** | { **viewname** *mib-view* }]
显示系统联络字符串	**display snmp-agent sys-info contact**
显示系统位置字符串	**display snmp-agent sys-info location**
显示系统启用的 SNMP 版本	**display snmp-agent sys-info version**

5.5 SNMP 配置举例

1. 组网需求

网管工作站（NMS）与以太网交换机通过以太网相连，网管工作站 IP 地址为 129.102.149.23，以太网交换机的 VLAN 接口 IP 地址为 129.102.0.1。在交换机上进行如下配置：设置团体名和访问权限、管理员标识、联系方法以及交换机的位置信息、允许交换机发送 Trap 消息。

2. 组网图

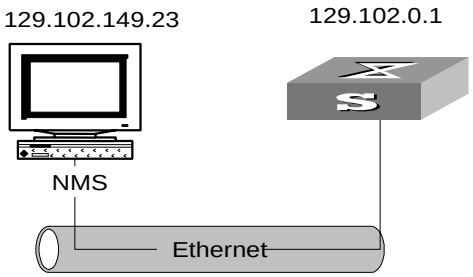


图5-2 SNMP 配置举例组网图

3. 配置步骤

进入系统视图

<Quidway>system-view

设置团体、群组和用户：

[Quidway] snmp-agent sys-info version all

[Quidway] snmp-agent community write public

[Quidway] snmp-agent mib include internet 1.3.6.1

[Quidway] snmp-agent group v3 managev3group write internet

[Quidway] snmp-agent usm v3 managev3user managev3group

设置网管使用的 VLAN 接口为 VLAN 2 接口，将用于网管的端口 GigabitEthernet0/3 加入到 VLAN2 中，配置 VLAN2 的接口 IP 地址 129.102.0.1。

[Quidway] vlan 2

[Quidway-vlan2] port gigabitethernet 0/3

[Quidway-vlan2] interface vlan 2

[Quidway-Vlan-interface2] ip address 129.102.0.1 255.255.255.0

允许向网管工作站（NMS）129.102.149.23 发送 Trap 报文，使用的团体名为 public。

[Quidway] snmp-agent trap enable standard authentication

[Quidway] snmp-agent trap enable standard coldstart

[Quidway] snmp-agent trap enable standard linkup

[Quidway] snmp-agent trap enable standard linkdown

[Quidway] snmp-agent target-host trap address udp-domain 129.102.149.23 udp-port 5000 params securityname public

4. 配置 NMS

网管所在的 PC 机需要进行登录设置。对于 Mib-Browser，登陆设置为：SNMPV1、V2 使用缺省的团体名 public 登录，SNMPV3 使用用户 managev3user 登陆。

以太网交换机支持华为公司的 iManager Quidview 网管系统。用户可利用网管系统完成对以太网交换机的查询和配置操作，具体情况请参考华为公司网管产品的配套手册。

第6章 RMON 配置

6.1 RMON 简介

RMON（Remote Monitoring）是 IETF（Internet Engineering Task Force）定义的一种 MIB，是对 MIB II 标准最重要的增强。RMON 主要用于对一个网段乃至整个网络中数据流量的监视，是目前应用相当广泛的网络管理标准之一。

RMON 的实现完全基于 SNMP 体系结构（这是它的一个突出优点），它与现存的 SNMP 框架相兼容，不需对该协议进行任何修改。RMON 包括 NMS 和运行在各网络设备上的 Agent 两部分。RMON Agent 在网络监视器或网络探测器上，跟踪统计其端口所连接的网段上的各种流量信息（如某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等）。RMON 使 SNMP 更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效的手段。RMON 能够减少网管站同代理间的通讯流量，从而可以简便而有力地管理大型互连网络。

RMON 允许有多个监控者，它可用两种方法收集数据：

- 一种方法利用专用的 RMON probe（探测仪）收集数据，NMS 直接从 RMON probe 获取管理信息并控制网络资源。这种方式可以获取 RMON MIB 的全部信息；
- 第二种方法是将 RMON Agent 直接植入网络设备（路由器、交换机、HUB 等）使它们成为带 RMON probe 功能的网络设施。RMON NMS 使用 SNMP 的基本命令与 SNMP Agent 交换数据信息，收集网络管理信息，但这种方式受设备资源限制，一般不能获取 RMON MIB 的所有数据，大多数只收集四个组的信息。这四个组是：报警信息、事件信息、历史信息和统计信息。

以太网交换机以第二种方法实现 RMON。通过运行在网络监视器上的支持 RMON 的 SNMP Agent，网管站可以获得与被管网络设备端口相连的网段上的整体流量、错误统计和性能统计等信息，进而实现对网络（往往是远程的）的管理。

6.1 配置 RMON

> 说明：
> 在配置RMON功能之前，必须保证SNMP agent已经正确配置。SNMP agent的配置请参见 第 5 章　SNMP配置。

RMON 配置包括：

- 添加/删除事件表的一个表项
- 添加/删除告警表的一个表项
- 添加/删除扩展 RMON 告警表的一个表项
- 添加/删除历史控制表的一个表项
- 添加/删除统计表的一个表项

6.1.1 添加/删除事件表的一个表项

本配置用来定义事件号及事件的处理方式。事件有如下几种处理方式：

- 将事件记录在日志表中
- 向网管站发 Trap 消息
- 将事件记录在日志表中并向网管站发 Trap 消息

请在系统视图下进行下列配置。

表6-1 在事件表中添加/删除一个表项

操作	命令
在事件表中添加一个表项	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]
在事件表中删除一个表项	**undo rmon event** *event-entry*

6.1.2 添加/删除告警表的一个表项

RMON 告警管理可对指定的告警变量（如端口的统计数据）进行监视，当被监视数据的值超过定义的阈值时会产生告警事件，然后按照事件的定义进行相应的处理。事件的定义在事件管理中实现。

📖 **说明：**

在添加告警表项之前，需要通过 rmon event 命令定义好告警表项中引用的事件。

请在系统视图下进行下列配置。

表6-2 在告警表中添加/删除一个表项

操作	命令
在告警表中添加一个表项	**rmon alarm** *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]
在告警表中删除一个表项	**undo rmon alarm** *entry-number*

用户定义了告警表项后，系统对告警表项的处理如下：

（1）对所定义的告警变量 *alarm-variable* 按照定义的时间间隔 *sampling-time* 进行采样

（2） 将采样值和设定的阈值进行比较，按照下表执行相应的处理过程

表6-3 告警表项的处理过程

实际情况	处理过程
采样值大于等于设定的上限 *threshold-value1*	触发所定义的事件 *event-entry1*
采样值大于设定的下限 *threshold-value2*	触发所定义的事件 *event-entry2*

6.1.3 添加/删除扩展 RMON 告警表的一个表项

该命令用来在扩展 RMON 告警表中添加/删除一行表项。扩展告警表项可以对告警变量的采样值进行运算，然后将运算结果和设置的阈值比较，实现更为丰富的告警功能。

📖 **说明：**

在添加扩展告警表项之前，需要通过 rmon event 命令定义好告警表项中引用的事件。

请在系统视图下进行下列配置。

表6-4 在扩展 RMON 告警表中添加/删除一个表项

操作	命令
在扩展 RMON 告警表中添加一个表项	**rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-timer* { **delta | absolute | changeratio** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever | cycle** *cycle-period* } [**owner** *text*]
在扩展 RMON 告警表中删除一个表项	**undo rmon prialarm** *entry-number*

用户定义了扩展告警表项后，系统对告警表项的处理如下：

（1） 对定义的扩展告警公式 *prialarm-formula* 中的告警变量按照定义的时间间隔 *sampling-timer* 进行采样

（2） 将采样值按照定义的运算公式 *prialarm-formula* 进行计算

（3） 将计算结果和和设定的阈值进行比较，按照下表执行相应的处理过程

表6-5 扩展告警表项的处理过程

实际情况	处理过程
计算值大于等于设定的上限 *threshold-value1*	触发所定义的事件 *event-entry1*
计算值大于等于设定的下限 *threshold-value2*	触发所定义的事件 *event-entry2*

6.1.4 添加/删除历史控制表的一个表项

利用历史数据管理功能，可以对设备进行设置，设置的任务包括：采集历史数据、定期采集并保存指定端口的数据。抽样信息包括利用率、错误数和总包数等。

可以使用下面的命令在历史控制表中添加/删除一个表项。

请在以太网端口视图进行下列配置。

表6-6 在历史控制表中添加/删除一个表项

操作	命令
在历史控制表中添加一行	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text-string*]

在历史控制表中删除一行	**undo rmon history** *entry-number*

历史控制表项统计的是采样时间间隔内的各种数据的统计值。用户可以通过 **display rmon history** 命令来显示历史控制表项的信息。

6.1.5 添加/删除统计表的一个表项

利用 RMON 统计管理功能，可以监视端口的使用情况、统计端口使用中发生的错误。统计信息包括冲突、循环冗余校验和队列、过小（或超大）的数据包、超时传送、碎片、广播、多播、单播消息以及带宽使用效率等。

可以使用下面的命令在统计表中添加/删除一个表项。

请在以太网端口视图下进行下列配置。

表6-7 在统计表中添加/删除一个表项

操作	命令
在统计表中添加一行	**rmon statistics** *entry-number* [**owner** *text-string*]
在统计表中删除一行	**undo rmon statistics** *entry-number*

统计表项统计的是从该事件定义的时间开始的一个累计的信息。用户可以通过 **display rmon statistics** 命令来显示统计表项的信息。

6.2 RMON 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 RMON 的运行情况，通过查看显示信息验证配置的效果。

表6-8 RMON 显示和调试

操作	命令
显示 RMON 统计消息	**display rmon statistics** [port-num]
显示 RMON 历史信息	**display rmon history** [*port-num*]
显示 RMON 告警信息	**display rmon alarm** [*alarm-table-entry*]
显示扩展 RMON 告警信息	**display rmon prialarm** [*prialarm-table-entry*]
显示 RMON 事件	**display rmon event** [*event-table-entry*]
显示 RMON 事件日志	**display rmon eventlog** [*event-number*]

6.3 RMON 配置举例

1. 组网需求

在 RMON 以太网统计表中设定一个表项，进行以太网端口性能统计，以便网管查询。

2. 组网图

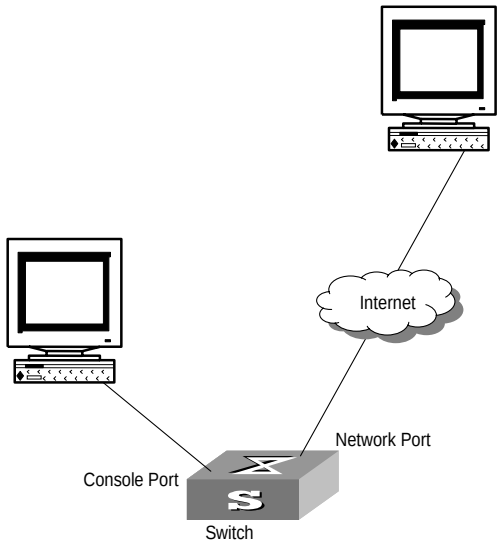


图6-1 配置 RMON 组网图

3. 配置步骤

配置 RMON。

[Quidway-Ethernet2/1] rmon statistics 1 owner huawei-rmon

在用户视图下查看 RMON 配置。

<Quidway> display rmon statistics ethernet 2/1

```
Statistics entry 1 owned by huawei-rmon is VALID.
  Gathers statistics of interface Ethernet2/1. Received:
  octets               : 270149  , packets            : 1954
  broadcast packets   :1570    , multicast packets :365
  undersized packets  :0         , oversized packets:0
  fragments packets   :0         , jabbers packets   :0
  CRC alignment errors:0         , collisions        :0
  Dropped packet events (due to lack of resources):0
  Packets received according to length (in octets):
```

```
64     :644       ,  65-127  :518       ,  128-255  :688
256-511:101      ,  512-1023:3         ,  1024-1518:0
```

第7章　NTP 配置

7.1　NTP 简介

7.1.1　NTP 的作用

随着网络拓扑的日益复杂，整个网络内设备的时钟同步将变得十分重要。NTP（Network Time Protocol）就是用来在整个网络内发布精确时间的 TCP/IP 协议。

NTP 可以为以下应用提供一致性保证：

- 在备份服务器和客户机之间进行增量备份时，确保这两个系统之间的时钟同步。
- 当由多个系统来处理复杂的事件时，确保多个系统参考同一时钟，保证事件的正确顺序。
- 确保系统之间的 RPC（远程系统调用）能够正常进行。
- 为应用程序提供用户登录到系统、文件的修改等操作的时间信息。

7.1.2　NTP 的基本工作原理

NTP 的基本工作原理如下图所示：

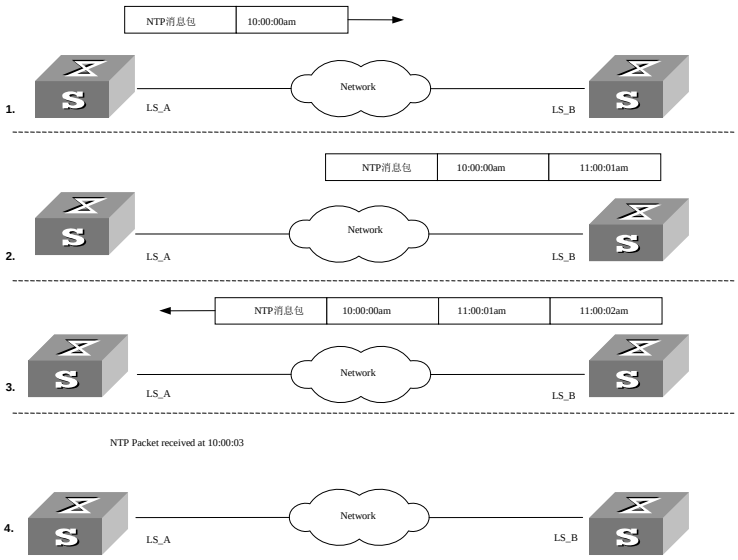


图7-1　NTP 基本原理图

上图中，以太网交换机 A 和以太网交换机 B 通过串口相连，它们都有自己独立的系统时钟，要实现各自系统时钟的自动同步，作如下假设：

- 在以太网交换机 A 和 B 的系统时钟同步之前，以太网交换机 A 的时钟设定为 10:00:00am，以太网交换机 B 的时钟设定为 11:00:00am。
- 以以太网交换机 B 为 NTP 时间服务器，即以太网交换机 A 将使自己的时钟与以太网交换机 B 的时钟同步。
- 数据包在以太网交换机 A 和 B 之间单向传输所需要的时间为 1 秒。

系统时钟同步的工作过程如下：

- 以太网交换机 A 发送一个 NTP 消息包给以太网交换机 B，该消息包带有它离开以太网交换机 A 时的时间戳，该时间戳为 10:00:00am（T_1）。
- 当此 NTP 消息包到达以太网交换机 B 时，以太网交换机 B 加上自己的时间戳，该时间戳为 11:00:01am（T_2）。
- 当此 NTP 消息包离开以太网交换机 B 时，以太网交换机 B 再加上自己的时间戳，该时间戳为 11:00:02am（T_3）。
- 当以太网交换机 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（T_4）。

至此，以太网交换机 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=（T_4-T_1）-（T_3-T_2）。
- 以太网交换机 A 相对以太网交换机 B 的时间差 offset=（（T_2-T_1）+（T_3-T_4））/2。

这样以太网交换机 A 就能够根据这些信息来设定自己的时钟，使之与以太网交换机 B 的时钟同步。

以上内容只是对 NTP 的工作原理的粗略描述，详细内容请参阅 RFC1305。

7.2 NTP 协议配置

NTP 协议用于整个网络内的时间同步，NTP 配置包括：

- 配置 NTP 工作模式
- 设置 NTP 身份验证功能
- 设置 NTP 验证密钥
- 设置指定密钥为可信密钥
- 设置本地发送 NTP 消息的接口
- 设置外部参考时钟或本地时钟作为 NTP 主时钟

- 允许/禁止接口接收 NTP 消息
- 设置对本地以太网交换机服务的访问控制权限
- 设置本地允许建立的 sessionss 的数目

7.2.1 配置 NTP 工作模式

根据以太网交换机在网络中的位置以及网络结构，可设置本地以太网交换机在 NTP 协议中的工作模式，例如可以设置远程服务器为本地时间服务器，此时本地以太网交换机工作在 client 模式；也可以设置远程服务器作为本地以太网交换机的对等体，本地运行在 symmetric active 模式；也可以设置本地以太网交换机的一个接口发送 NTP 的广播消息包，此时本地以太网交换机工作在 broadcast 模式；也可以设置本地以太网交换机的一个接口接收 NTP 的广播信息包，此时本地以太网交换机工作在广播客户模式；也可以设置本地以太网交换机的一个接口发送 NTP 组播消息包，本地以太网交换机运行在 multicast 模式；还可以设置本地以太网交换机的一个接口接收 NTP 组播消息包，本地以太网交换机运行在组播客户模式。

- 配置 NTP 服务器模式
- 配置 NTP 对等体模式
- 配置 NTP 广播服务器模式
- 配置 NTP 广播客户模式
- 配置 NTP 组播服务器模式
- 配置 NTP 组播客户模式

配置 NTP 服务器模式

设置以 *ip-address* 所指定的远程服务器作为本地时间服务器。*ip-address* 是一个主机地址，不能为广播、组播地址或参考时钟的 IP 地址。本地以太网交换机工作在 client 模式，在这种工作模式下，只能是本地客户机同步到远程服务器，而远程服务器不会同步到本地客户机。

请在系统视图下进行下列配置。

表7-1 配置 NTP 时间服务器

操作	命令
配置 NTP 时间服务器	**n ntp-service unicast-server** *ip-address* [**version** *number*] [**authentication-keyid** *keyid*] [**source-interface** { *interface-name* | *interface-type interface-number* }] [**priority**] *
取消 NTP 服务器模式	**undo ntp-service unicast-server** *ip-address*

NTP 版本号 *number* 范围是 1～3，缺省值为 3；身份验证密钥 ID 号 *keyid* 范围为 0 ～ 4294967295；接口 *interface-name* 或 *interface-type interface-number* 指定本地以太网交换机给时间服务器发送 NTP 消息时，消息包中的源 IP 地址从该接口获取；**priority** 指定该时间服务器为优先选择的时间服务器。

配置 NTP 对等体模式

设置以 *ip-address* 所指定的远程服务器作为本地的对等体，本地运行在 symmetric active 模式。*ip-address* 是一个主机地址，不能为广播、组播地址或参考时钟的 IP 地址。在这种配置下，本地以太网交换机能同步到远程服务器，远程服务器也能同步到本地服务器。

请在系统视图下进行下列配置。

表7-2 配置 NTP 对等体模式

操作	命令
配置 NTP 对等体模式	**ntp-service unicast-peer** *ip-address* [**version** *number*] [**authentication-key** *keyid*] [**source-interface** { *interface-name* | *interface-type interface-number* }] [**priority**] *
取消 NTP 对等体模式	**undo ntp-service unicast-peer** *ip-address*

NTP 版本号 *number* 范围是 1～3，缺省值为 3；身份验证密钥 ID 号 *keyid* 范围为 0 ～ 4294967295；接口 *interface-name* 或 *interface-type interface-number* 指定本地以太网交换机给对等体发送 NTP 消息时，消息包中的源 IP 地址从该接口获取；**priority** 指定该对等体为优先选择的时间服务器。

配置 NTP 广播服务器模式

指定本地以太网交换机上的一个接口来发送 NTP 广播消息包，本地运行在 broadcast 模式，作为广播服务器周期性地发送广播消息到广播客户端。

请在 VLAN 接口视图下进行下列配置。

表7-3 配置 NTP 广播服务器模式

操作	命令
配置 NTP 广播服务器模式	**ntp-service broadcast-server** [**authentication-keyid** *keyid* **version** *number*] *
取消 NTP 广播服务器模式	**undo ntp-service broadcast-server**

NTP 版本号 *number* 范围是 1～3，缺省值为 3；身份验证密钥 ID 号 *keyid* 范围 0～4294967295；此命令必须在欲发送 NTP 广播消息包的接口下配置。

配置 NTP 广播客户模式

指定本地以太网交换机上的某接口来接收 NTP 广播消息包，并运行在广播客户模式。本地以太网交换机首先侦听来自服务器的广播消息包，当接收到第一个广播消息包时，本地以太网交换机为了估计网络延迟先启用一个短暂的 client/server 模式与远程服务器交换消息，然后本地以太网交换机就进入广播客户模式，继续侦听广播消息包的到来，根据到来的广播消息包对本地时钟进行同步。

请在 VLAN 接口视图下进行下列配置。

表7-4 配置 NTP 广播客户模式

操作	命令
配置 NTP 广播客户模式	**ntp-service broadcast-client**
取消 NTP 广播客户模式	**undo ntp-service broadcast-client**

此命令必须在欲接收 NTP 广播消息包的接口下配置。

配置 NTP 组播服务器模式

指定本地以太网交换机上的一个接口来发送 NTP 组播消息包，本地运行在 multicast 模式，作为组播服务器周期性地发送组播消息到组播客户端。

请在 VLAN 接口视图下进行下列配置。

表7-5 配置 NTP 组播服务器模式

操作	命令
配置 NTP 组播服务器模式	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid*] [**ttl** *ttl-number*] [**version** *number*]
取消 NTP 组播服务器模式	**undo ntp-service multicast-server**

NTP 版本号 *number* 范围是 1～3，缺省值为 3；身份验证密钥 ID 号 *keyid* 范围 0～4294967295；组播包的生存期 *ttl-number* 范围为 1～255；组播 IP 地址缺省为 224.0.1.1；

此命令必须在欲发送 NTP 组播消息包的接口下配置。

配置 NTP 组播客户模式

指定本地以太网交换机上的接口来接收 NTP 组播消息包，本地以太网交换机运行在组播客户模式。本地以太网交换机首先侦听来自服务器的组播消息包，当接收到第一个组播消息包时，本地以太网交换机为了估计网络延迟先启用一个短暂的 client/server 模式与远程服务器交换消息，然后本地以太网交换机就进入组播客户模式，继续侦听组播消息包的到来，根据到来的组播消息包对本地时钟进行同步。

请在 VLAN 接口视图下进行下列配置。

表7-6 配置 NTP 组播客户模式

操作	命令
配置 NTP 组播客户模式	**ntp-service multicast-client** [*ip-address*]
取消配置 NTP 组播客户模式	**undo ntp-service multicast-client**

组播 IP 地址 *ip-address* 缺省为 224.0.1.1；此命令必须在欲接收 NTP 组播消息包的接口下配置。

7.2.2 配置 NTP 身份验证功能

启动 NTP 身份验证功能，设置 MD5 身份验证密钥，并指定可信密钥。client 只会同步到提供可信密钥的服务器，如果服务器提供的密钥不是可信的密钥，那么 client 不会与其同步。

请在系统视图下进行下列配置。

表7-7 配置 NTP 身份验证功能

操作	命令
启动 NTP 身份验证功能	**ntp-service authentication enable**
停止 NTP 身份验证功能	**undo ntp-service authentication enable**

7.2.3 设置 NTP 验证密钥

该配置任务用来设置 NTP 验证密钥。

请在系统视图下进行下列配置。

表7-8 配置 NTP 验证密钥

操作	命令
设置 NTP 验证密钥	**ntp-service authentication-keyid** *number* **authentication-mode md5** *value*
取消 NTP 验证密钥	**undo ntp-service authentication-keyid** *number*

密钥编号 *number* 范围为 1～4294967295；密钥值 *value* 为 1～32 个 ASCII 码字符。

7.2.4 设置指定密钥为可信密钥

该配置任务用来指定密钥是可信的。

请在系统视图下进行下列配置。

表7-9 设置指定密钥为可信密钥

操作	命令
指定密钥是可信的	**ntp-service reliable authentication-keyid** *key-number*
取消指定可信密钥	**undo ntp-service reliable authentication-keyid** *key-number*

密钥编号 *key-number* 范围为 1～4294967295。

7.2.5 设置本地发送 NTP 消息的接口

指定本地发送所有 NTP 消息时，消息包中的源 IP 地址都用一个特定 IP 地址，该 IP 地址就是从所指定的接口上获取。

请在系统视图下进行下列配置。

表7-10 设置本地发送 NTP 消息的接口

操作	命令
设置本地发送 NTP 消息的接口	**ntp-service source-interface** { *interface-name* | *interface-type interface-number* }
取消设置本地发送 NTP 消息的接口	**undo ntp-service source-interface**

接口由 *interface-name* 或 *interface-type interface-number* 确定，消息包中的源 IP 地址从该接口获取，如果 **ntp-service unicast-server** 或 **ntp-service**

unicast-peer 中也指定了发送接口，则以 **ntp-service unicast-server** 或 **ntp-service unicast-peer** 指定的为准。

7.2.6 设置 NTP 主时钟

该配置任务用来设置外部参考时钟或本地时钟作为 NTP 主时钟。

请在系统视图下进行下列配置。

表7-11 设置外部参考时钟或本地时钟作为 NTP 主时钟

操作	命令
设置外部参考时钟或本地时钟作为 NTP 主时钟	**ntp-service refclock-master** [*ip-address*] [*stratum*]
取消 NTP 主时钟设置	**undo ntp-service refclock-master** [*ip-address*]

ip-address 是参时钟 IP 地址 127.127.t.u，其中 t 的取值范围为 0～37、u 的取值范围为 0～3；*stratum* 用来指定本地时钟所处的层数，范围为 1～15。当不指定 IP 地址时，默认设置本地时钟为 NTP 主时钟；可以指定 NTP 主时钟所处的层次数。

7.2.7 设置禁止/允许接口接收 NTP 消息

该配置任务用来设置禁止或允许接口接收 NTP 消息。

请在 VLAN 接口视图下进行下列配置。

表7-12 设置禁止/允许接口接收 NTP 消息

操作	命令
设置禁止接口接收 NTP 消息	**ntp-service in-interface disable**
设置允许接口接收 NTP 消息	**undo ntp-service in-interface disable**

该配置任务必须在需要禁止接收 NTP 消息的接口下配置。

7.2.8 设置对本地以太网交换机服务的访问控制权限

设置对本地以太网交换机 NTP 服务的访问控制权限。这里提供了一种最小限度的安全措施，更安全的方法是进行身份验证。当有一个访问请求时，按照最小访问限制到最大访问限制依次匹配，以第一个匹配的为准，匹配顺序为 **peer**、**serve**、**serve only**、**query only**。

请在系统视图下进行下列命令的操作。

表7-13 设置对本地以太网交换机服务的访问控制权限

操作	命令
设置对本地以太网交换机服务的访问控制权限	**ntp-service access** { **query** | **synchronization** | **serve** | **peer** } *acl-number*
取消设置对本地以太网交换机服务的访问控制权限	**undo ntp-service access** { **query** | **synchronization** | **serve** | **peer** }

IP 地址访问列表标号 *acl-number* 范围为 2000～2999。其它访问权限含义为：

query：只允许对本地 NTP 服务进行控制查询。

synchronization：只允许对本地 NTP 服务进行时间请求。

serve：可以对本地 NTP 服务进行时间请求和控制查询，但本地时钟不会同步到远程服务器。

peer：既可以对本地 NTP 服务进行时间请求和控 制查询，本地时钟又可以同步到远程服务器。

7.2.9 设置本地允许建立的 sessions 数目

该配置任务用来设置本地允许建立的 sessions 的数目。

请在系统视图下进行下列配置。

表7-14 设置本地允许建立的 sessions 数目

操作	命令
设置本地允许建立的 sessions 数目	**ntp-service max-dynamic-sessions** *number*
恢复本地允许建立的 sessions 数目为缺省值	**undo ntp-service max-dynamic-sessions**

本地允许建立 sessions 的数目 *number*，范围 0～100，缺省值为 100。

7.3 NTP 显示与调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 NTP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可对 NTP 进行调试。

表7-15 NTP 显示与调试

操作	命令
显示 NTP 服务的状态信	**display ntp-service status**
显示 NTP 服务维护的 sessions 状态	**display ntp-service sessions** [**verbose**]
显示从本地设备回溯到参考时钟源的各个 NTP 时间服务器的简要信息。	**display ntp-service trace** [*ip-address*]
打开 NTP 的调试开关	**debugging ntp-service**

7.4 NTP 典型配置举例

1. 配置 NTP 服务器

(1)　组网需求

Quidway1 设置本地时钟作为 NTP 主时钟，层数为 2，Quidway2 以 Quidway1 作为时间服务器，将其设为 server 模式，自己为 client 模式。

(2)　组网图

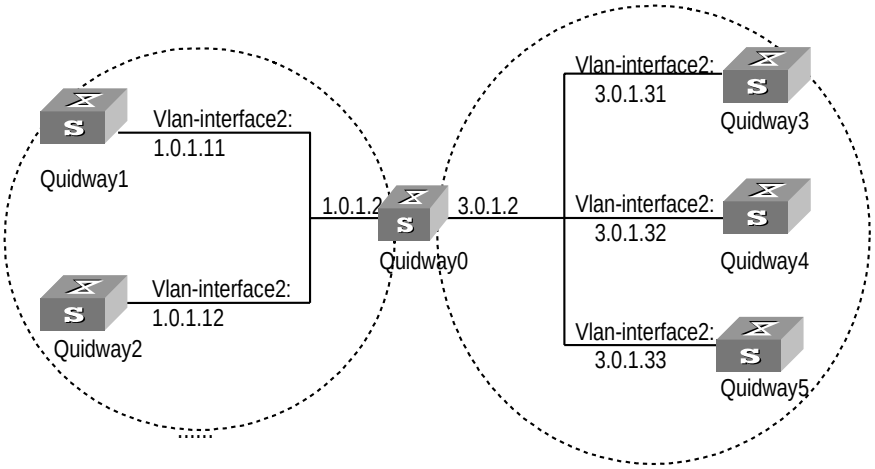


图7-2 NTP 典型配置的组网图

(3)　配置步骤

配置以太网交换机 Quidway1：

进入系统视图。

<Quidway1> system-view

设置本地时钟作为 NTP 主时钟，层数为 2。

[Quidway1] ntp-service refclock-master 2

配置以太网交换机 Quidway2：

进入系统视图。

<Quidway2> system-view

设置 Quidway1 为时间服务器。

[Quidway2] ntp-service unicast-server 1.0.1.11

以上配置将 Quidway2 向 Quidway1 进行时间同步，同步前观察 Quidway2 的状态为：

[Quidway2] display ntp-service status

```
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 99.8562 Hz, actual freq is 99.8562 Hz, precision is 2**7
reference time is 00000000.00000000(00:00:00.000 UTC Jan  1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
```

同步后观测 Quidway2 的状态为：

[Quidway2] display ntp-service status

```
Clock is synchronized, stratum 3, reference is 1.0.1.11
nominal freq is 250.0000 Hz, actual freq is 249.9992 Hz, precision is
2**19
reference time is BF422AE4.05AEA86C (17:03:32.022 UTC Thu Sep 6 2001)
clock offset is 198.7425 msec, root delay is 27.47 msec
root dispersion is 208.39 msec, peer dispersion is 9.63 msec
```

此时 Quidway2 已经与 Quidway1 同步，层数比 Quidway1 大 1，为 3。

观察 Quidway2 的 sessions 情况，Quidway2 与 Quidway1 建立了连接。

[Quidway2] display ntp-service sessions

```
address ref clock     st  when  poll reach  delay  offset    disp
*~1.0.1.11 127.127.7.1    3    1    64  377    26.1    199.53    9.7
* master (synced), # master (unsynced), + selected, - candidate, ~
configured
```

配置 NTP 对等体举例

(4)　组网需求

Quidway3 设置本地时钟作为 NTP 主时钟，层数为 2，Quidway4 以 Quidway3 作为时间服务器，将其设为 server 模式，自己为 client 模式。同时，Quidway5 将 Quidway4 设为对等体。

(5)　组网图

如图 7-2 所示。

(6)　配置步骤

配置以太网交换机 Quidway3：

进入系统视图。

<Quidway3> system-view

设置本地时钟作为 NTP 主时钟，层数为 2。

[Quidway3] ntp-service refclock-master 2

配置以太网交换机 Quidway4：

进入系统视图。

<Quidway4> system-view

设置 Quidway3 为时间服务器，同步后层数为 3。

[Quidway4] ntp-service unicast-server 3.0.1.31

配置以太网交换机 Quidway5：(Quidway4 已经向 Quidway3 同步后）

进入系统视图。

<Quidway5> system-view

设置本地时钟作为 ntp 主时钟，层数为 1。

[Quidway5] ntp-service refclock-master 1

本地同步后，设置 Quidway4 位对等体。

[Quidway5] ntp-service unicast-peer 3.0.1.32

以上配置将 Quidway4 和 Quidway5 配置为对等体，Quidway5 处于主动对等体模式，Quidway4 处于被动对等体模式，由于 Quidway5 的层数为 1，而 Quidway4 的层数为 3，所以 Quidway4 向 Quidway5 同步。

同步后观测 Quidway4 的状态为：

[Quidway4] display ntp-service status

```
Clock is synchronized, stratum 2, reference is 3.0.1.33
nominal freq is 250.0000 Hz, actual freq is 249.9992 Hz, precision is
2**19
reference time is BF422AE4.05AEA86C (17:03:32.022 UTC Thu Sep 6 2001)
clock offset is 198.7425 msec, root delay is 27.47 msec
root dispersion is 208.39 msec, peer dispersion is 9.63 msec
```

此时 Quidway4 已经与 Quidway5 同步，层数比 Quidway5 大 1，为 2。

观察 Quidway4 的 sessions 情况，Quidway4 与 Quidway5 建立了连接。

[Quidwa4] display ntp-service sessions

```
address  ref clock     st  when  poll reach  delay  offset    disp
*3.0.1.33  127.127.7.1   3     1   64   377    26.1    199.53    9.7
* master (synced), # master (unsynced), + selected, - candidate, ~
configured
```

配置 NTP 广播模式

(7)　组网需求

Quidway3 设置本地时钟作为 NTP 主时钟，层数为 2，并从接口 Vlan-interface2 向外发送广播消息包，设置 Quidway4 和 Quidway1 分别从各自的接口 Vlan-interface2 监听广播消息。

(8)　组网图

如图 7-2 所示。

(9)　配置步骤

配置以太网交换机 Quidway3：

进入系统视图。

<Quidway3> system-view

设置本地时钟作为 NTP 主时钟，层数为 2。

[Quidway3] ntp-service refclock-master 2

进入接口 Vlan-interface2 视图。

[Quidway3] interface vlan-interface 2

设置为广播服务器。

[Quidway3-Vlan-Interface2] ntp-service broadcast-server

配置以太网交换机 Quidway4：

进入系统视图。

<Quidway4> system-view

进入接口 Vlan-interface2 视图。

[Quidway4] interface vlan-interface 2

[Quidway4-Vlan-Interface2] ntp-service broadcast-client

配置以太网交换机 Quidway1：

进入系统视图。

<Quidway1> system-view

进入接口 Vlan-interface2 视图。

[Quidway1] interface vlan-interface 2

[Quidway1-Vlan-Interface2] ntp-service broadcast-client

以上配置将 Quidway4 和 Quidway1 配置为从接口 Vlan-interface2 监听广播消息，而 Quidway3 从接口 Vlan-interface2 发送广播消息包，由于 Quidway1 与 Quidway3 不在相同的网段，所以接收不到 Quidway3 发出的广播包，而 Quidway4 接收到 Quidway3 发出的广播包后与其同步。

同步后观测 Quidway4 的状态为：

[Quidway4] display ntp-service status

```
clock status: synchronized
 clock stratum: 8
 reference clock ID: LOCAL(0)
 nominal frequency: 100.0000 Hz
 actual frequency: 100.0000 Hz
 clock precision: 2^17
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 10.94 ms
 peer dispersion: 10.00 ms
 reference time: 20:54:25.156 UTC Mar 7 2002(C0325201.2811A112)
```

此时 Quidway4 已经与 Quidway3 同步，层数比 Quidway3 大 1，为 3。

观察 Quidway4 的 sessions 情况，Quidway4 与 Quidway3 建立了连接。

[Quidway2] display ntp-service sessions

```
  source        reference      stra reach poll  now offset  delay disper
**************************************************************************
[12345]127.127.1.0    LOCAL(0)       7   377   64   57   0.0    0.0    1.0
[5]1.0.1.11        0.0.0.0        16     0   64    -    0.0    0.0    0.0
[5]128.108.22.44   0.0.0.0         16     0   64    -    0.0    0.0    0.0
note:  1  source(master),2  source(peer),3  selected,4  candidate,5
configured
```

配置 NTP 组播模式

(10) 组网需求

Quidway3 设置本地时钟作为 NTP 主时钟，层数为 2，并从接口 Vlan-interface2 向外发送组播消息包，设置 Quidway4 和 Quidway1 分别从各自的接口 Vlan-interface2 监听组播消息。

(11) 组网图

如图 7-2 所示。

(12) 配置步骤

配置以太网交换机 Quidway3：

进入系统视图。

<Quidway3> system-view

设置本地时钟作为 NTP 主时钟，层数为 2。

[Quidway3] ntp-service refclock-master 2

进入接口 Vlan-interface2 的视图。

[Quidway3] interface vlan-interface 2

设置为组播服务器。

[Quidway3-Vlan-Interface2] ntp-service multicast-server

配置以太网交换机 Quidway4：

进入系统视图。

<Quidway4> system-view

进入接口 Vlan-interface2 的视图。

[Quidway4] interface vlan-interface 2

设置为组播客户模式。

[Quidway4-Vlan-Interface2] ntp-service multicast-client

配置以太网交换机 Quidway1：

进入系统视图。

<Quidway1> system-view

进入接口 Vlan-interface2 的视图。

[Quidway1] interface vlan-interface 2

设置为组播客户模式。

[Quidway1-Vlan-Interface2] ntp-service multicast-client

以上配置将 Quidway4 和 Quidway1 配置为从接口 Vlan-interface2 监听组播消息，而 Quidway3 从接口 Vlan-interface2 发送组播消息包，由于 Quidway1 与 Quidway3 不在相同的网段，所以接口不到 Quidway3 发出的组播包，而 Quidway4 接收到 Quidway3 发出的组播包后与其同步。

配置带身份验证的 NTP 服务器模式

(13) 组网需求

Quidway1 设置本地时钟作为 NTP 主时钟，层数为 2，Quidway2 以 Quidway1 作为时间服务器，将其设为 server 模式，自己为 client 模式，同时加入身份验证。

(14) 组网图

如图 7-2 所示。

(15) 配置步骤

配置以太网交换机 Quidway1：

进入系统视图。

<Quidway1> system-view

设置本地时钟作为 NTP 主时钟，层数为 2。

[Quidway1] ntp-service refclcok-master 2

配置以太网交换机 Quidway2：

进入系统视图。

<Quidway2> system-view

设置 Quidway1 为时间服务器。

[Quidway2[ntp-service unicast-server 1.0.1.11

启动身份验证。

[Quidway2] ntp-service authentication enable

设置密钥。

[Quidway2] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey

指定密钥为可信密钥。

[Quidway2] ntp-service reliable authentication-keyid 42

以上配置将 Quidway2 向 Quidway1 进行时间同步，由于 Quidway1 没有启动身份验证，所以 Quidway2 还是无法向 Quidway1 同步。现在在 Quidway1 增加以下配置:

启动身份验证。

[Quidway1] ntp-service authentication enable

设置密钥。

[Quidway1] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey

指定密钥为可信密钥。

[Quidway1] ntp-service reliable authentication-keyid 42

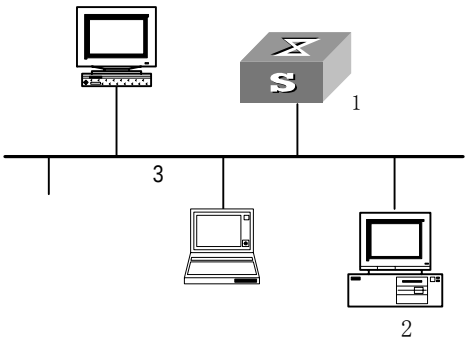
第8章 SSH 终端服务

8.1 SSH 终端服务

8.1.1 SSH 简介

SSH是Secure Shell（安全外壳）的简称，用户通过一个不能保证安全的网络环境远程登录到以太网交换机时，SSH特性可以提供安全的信息保障和强大的认证功能，以保护以太网交换机不受诸如IP地址欺诈、明文密码截取等等攻击。以太网交换机可以同时接受多个SSH客户的连接。SSH客户端的功能是允许用户与支持SSH Server的以太网交换机、UNIX主机等建立SSH连接。如图 8-1所示，可以建立SSH通道进行本地连接。

交换机目前支持的版本是 SSH 1.5 版本，交换机作为 SSH Server。



1: 运行 SSH server 的交换机　2: 运行 SSH client 的 PC　3: 以太网类型的局域网

图8-1 在局域网内建立 SSH 通道

📖 说明：

图中以太网端口所属的 VLAN 必须是已经创建了 VLAN 接口的 VLAN，同时 VLAN 接口上已经配置了 IP 地址。

整个通讯过程中，服务器端与客户端经历如下五个阶段：版本号协商阶段、密钥协商阶段、认证阶段、会话请求阶段、交互会话阶段，完成实现 SSH 的认证安全连接。

- 版本号协商阶段：客户端向服务器端发送 TCP 连接请求。TCP 连接建立后，服务器和客户端之间协商版本号。经过协商，如果服务器和客户

端可以共同工作，则进入密钥算法协商阶段；如果服务器和客户端不能共同工作，服务器端就会断开 TCP 连接。

- 密钥协商阶段：在本阶段，服务器和客户端将会协商密钥算法、计算会话密钥。服务器端随机生成服务器端的 RSA 密钥，然后将该密钥的公钥部分发送给客户端。客户端以服务器端发送过来的公钥、本地随机产生的随机数为参数计算出会话密钥，同时将用于计算会话密钥的那部分随机数使用服务器端的公钥加密，然后回送给服务器端。服务器端使用服务器端的私钥对客户端回送回来的数据进行解密，得到客户端的随机数，然后以服务器端的公钥、客户端回送的随机数为参数，使用和客户端同样的算法计算出会话密钥。这样，会话密钥不用在网上传送，服务器端和客户端就取得了相同的会话密钥。两端进行会话时都使用会话密钥进行加密和解密，保证了数据的安全。本阶段完成后进入认证阶段。
- 认证阶段：在获取了会话密钥后，服务器端将对客户端的用户进行认证。客户端向服务器端发送自己的用户名信息。如果服务器端配置了该用户并且配置了该用户不需要认证，则直接进入会话请求阶段，否则服务器会对该用户进行认证。在服务器启动对用户进行认证后，客户端将采用各种认证方法向服务器端进行认证，直到认证通过或者服务器由于超时断开连接。SSH 提供两种认证方法：口令认证和 RSA 认证。口令认证就是服务器端对客户端发送过来的用户名和口令与本地配置的用户名和口令进行比较，二者完全匹配的则通过认证。RSA 认证过程如下：服务器端配置了客户端用户的 RSA 公钥；客户端首先向服务器端发送自己 RSA 公钥的成员模数；服务器端对成员模数进行有效性认证，认证通过后产生一个随机数，使用客户端的 RSA 公钥加密后发送给客户端；服务器端和客户端都以此随机数和会话号作为参数计算出用于认证的数据；客户端将自己计算出来的认证数据回送给服务器；服务器端将客户端发送过来的认证数据和本地计算得到的认证数据进行比较，如果二者相同，而认证通过，否则认证失败。
- 会话请求阶段：认证通过后，客户端将向服务器端发送会话请求。服务器端成功处理请求后 SSH 进入交互会话阶段。
- 交互会话阶段：客户端和服务器端进行数据交互，直到双方结束会话。

SSH 对用户的会话报文进行了加密传送；会话密钥是随机产生的，会话密钥的交换过程也是加密进行的，并且 RSA 保证了会话密钥不在网上传送即完成了客户端和服务器端口的密钥交换。这样 SSH 最大限度的保证了客户端和服务器端之间的数据安全。同时如果客户端发送的用户名不存在，服务器端仍

然会启动认证过程，使客户端无法确定该用户是否存在，从而起到了保护用户名的作用。

8.1.2 SSH 服务器配置

SSH 的基本配置是 SSH 客户端能够成功连接 SSH 服务器（以太网交换机）的必要配置。SSH 的高级配置是根据具体需要调整 SSH 连接参数的配置。

SSH 的配置包括：

- 设置系统所支持的协议
- 配置和销毁本地 RSA 密钥对
- 为 SSH 用户配置认证方式
- 设置服务器密钥的更新时间
- 设置 SSH 认证超时时间
- 设置 SSH 认证重试次数
- 进入公共密钥视图和编辑密钥
- 为 SSH 用户分配公共密钥

1. 设置系统所支持的远程登录协议

由于系统缺省所支持的远程登录协议是 Telnet，而不是 SSH，所以要启用 SSH 首先必须设置系统所支持的远程登录协议为 SSH。

请在系统视图下进行下列配置。

表8-1 设置系统所支持的远程登录协议及最大连接数

操作	命令
设置系统所支持的远程登录协议及最大连接数	**protocol inbound** { **all** | **ssh** | **telnet** }

注意：

如果在该用户界面上配置支持的协议是 SSH，为确保登录成功，请您务必配置相应的认证方式为 **authentication-mode scheme**；若配置认证方式为 **authentication-mode password** 和 **authentication-mode none**，则 **protocol inbound ssh** 配置结果将失败。反之亦然，如果某用户界面已经配置成支持 SSH 协议，则在此用户界面上 **authentication-mode password** 和 **authentication-mode none** 的配置将失败。

2. 配置和销毁本地 RSA 密钥对

该配置任务用来产生本地主机密钥对，如果此时已经有了 RSA 密钥，系统提示是否替换原有密钥。本地的服务器密钥对由 SSH Server 动态生成。服务器密钥和主机密钥的最小长度为 512 位，最大长度为 2048 位。

请在系统视图下进行下列配置。

表8-2 配置和销毁本地 RSA 密钥对

操作	命令
产生本地 RSA 密钥对	**rsa local-key-pair create**
销毁本地 RSA 密钥对	**rsa local-key-pair destroy**

⚠ 注意：

成功完成 SSH 登录的首要操作是：配置并产生本地 RSA 密钥对。请您在进行其它 SSH 配置之前，必须执行 **rsa local-key-pair create** 命令，以生成本地密钥对。

此命令只需执行一遍，以太网交换机重启后不必再次执行。

3. 为 SSH 用户配置认证方式

该配置任务用来为 SSH 用户指定认证方式。对于新的用户，必须指定认证方式，否则无法登录。

请在系统视图下进行下列配置。

表8-3 为 SSH 用户配置认证方式

操作	命令
为 SSH 用户配置认证方式	**ssh user** *username* **authentication-type** { **password** | **rsa** | **all** }
取消指定用户的登录认证方式	**undo ssh user** *username* **authentication-type**

如果配置为 RSA 认证方式，则必须在交换机上配置客户端用户的 RSA 公钥，即进行后面的 7、8 序号标示的配置。

缺省情况下，未指定用户的登录认证方式，即无法登录。

4. 设置服务器密钥的更新时间

该配置任务用来设置服务器密钥的定时更新时间，更大限度的保证系统的 SSH 连接的安全性。

请在系统视图下进行下列配置。

表8-4 设置服务器密钥的更新时间

操作	命令
设置服务器密钥的更新时间	**ssh server rekey-interval** *hours*
恢复缺省的更新时间	**undo ssh server rekey-interval**

系统缺省不对服务器密钥进行更新。

5. 设置 SSH 认证超时时间

该配置任务用来设置 SSH 的认证超时时间。

请在系统视图下进行下列配置。

表8-5 设置 SSH 认证超时时间

操作	命令
设置 SSH 认证超时时间	**ssh server timeout** *seconds*
恢复 SSH 默认的认证超时时间	**undo ssh server timeout**

系统默认的认证超时时间为 60 秒。

6. 设置 SSH 认证重试次数

该配置任务用来设置 SSH 用户请求连接的认证重试次数，防止恶意猜测等非法行为。

请在系统视图下进行下列配置。

表8-6 设置 SSH 认证重试次数

操作	命令
设置 SSH 认证重试次数	**ssh server authentication-retries** *times*
恢复 SSH 默认的认证重试次数	**undo ssh server authentication-retries**

系统默认的认证重试次数为 3。

7. 进入公共密钥视图编辑密钥

该配置任务用来进入公共密钥视图，对客户端的公钥进行配置。

📖 **说明：**

本配置适用于对 SSH 用户采用 RSA 认证的情况。在交换机端配置的是客户端 SSH 用户的 RSA 公钥。而在客户端，需要为该 SSH 用户指定与 RSA 公钥对应的 RSA 私钥。

如果交换机上对 SSH 用户配置的认证方式为口令认证，则不必进行本配置。

请在系统视图下进行下列配置。

表8-7 公共密钥配置

操作	命令
进入公共密钥视图	**rsa peer-public-key** *key-name*
删除指定的公钥	**undo rsa peer-public-key** *key-name*

使用 **rsa peer-public-key** 命令进入公共密钥编辑视图后，使用 **public-key-code begin** 命令开始输入密钥数据。输入密钥数据时，字符之间可以有空格但系统将剔除所有空格。需要注意的是所配置的公钥必须是按公钥格式编码的十六进制字符串。使用 **public-key-code end** 命令结束公共密钥编辑并保存密钥。在保存之前要进行密钥合法性的检测，如果用户配置的公钥字符串中存在非法字符，本次配置的密钥数据就全部无效。

请在公共密钥视图下进行下列配置。

表8-8 开始/结束公共密钥编辑

操作	命令
进入公共密钥编辑视图	**public-key-code begin**
结束公共密钥编辑视图	**public-key-code end**

8. 为 SSH 用户分配公共密钥

该配置任务用来为 SSH 用户分配一个已经存在的公钥。

请在系统视图下进行下列配置。

表8-9 为 SSH 用户分配公钥

操作	命令
为 SSH 用户分配公钥	**ssh user** *username* **assign rsa-key** *keyname*
删除用户与公钥之间的对应关系	**undo ssh user** *username* **assign rsa-key**

8.1.3 SSH 客户端配置

SSH 客户端软件有很多，例如 PuTTY、FreeBSD 等。SSH 客户端要与服务器建立连接，在客户端上需要做连接的基本配置。一般来说，客户端需要的基本配置包括：

- 指定服务器 IP 地址。
- 选择远程连接协议为 SSH。通常客户端可以同上支持多种远程连接协议，如 Telnet、Rlogin、SSH 等。要建立 SSH 连接，必须选择远程连接协议为 SSH。
- 选择 SSH 版本。一般客户端都提供多种 SSH 版本选择。由于交换机目前支持的版本是 SSH Server 1.5 版本，客户端必须选择 1.5 或 1.5 以下版本。
- 指定 RSA 私钥文件。如果在服务器端配置了 SSH 用户采用 RSA 认证，就必须在客户端指定 RSA 私钥文件。RSA 密钥包括公钥和私钥。密钥文件一般是由客户端软件附带的工具生成的。其中公钥用来配置到服务器（以太网交换机）中，私钥应用在客户端中。

下面以第三方客户端软件 PuTTY 为例，说明 SSH 客户端的配置方法：

1. 指定服务器 IP 地址

打开 PuTTY 程序，出现如下客户端配置界面。

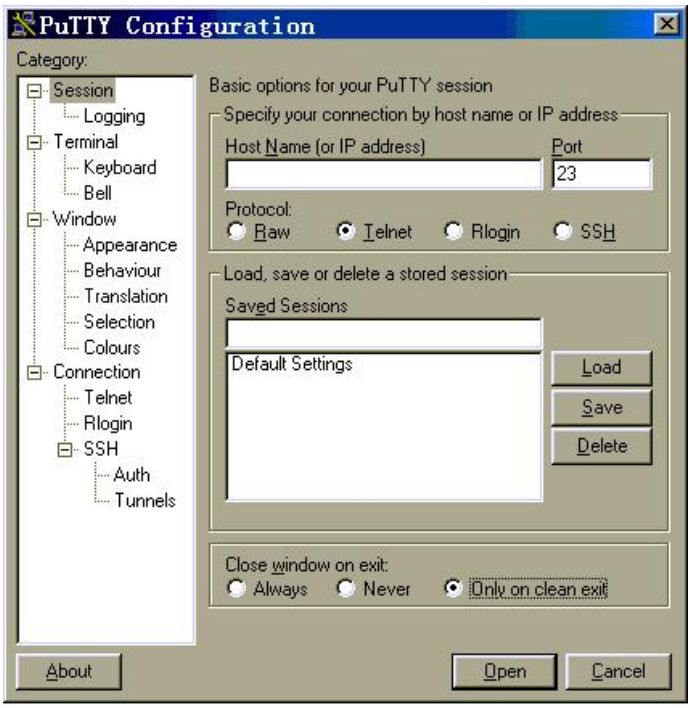


图8-2 SSH 客户端配置界面（1）

在“Host Name（or IP address）”文本框中输入以太网交换机 IP 地址（以太网交换机中任意一个协议“up”的接口的 IP 地址，但要求与 SSH 客户端主机的路由可达），如 10.110.28.10。

2. 选择远程连接协议为 SSH

如上图，在“Protocol”选择栏中选择“SSH”。

3. 选择 SSH 版本

单击 SSH 客户端配置界面左边目录项（“Category”）中的连接协议（“Connection”）中的“SSH”，出现如下界面：

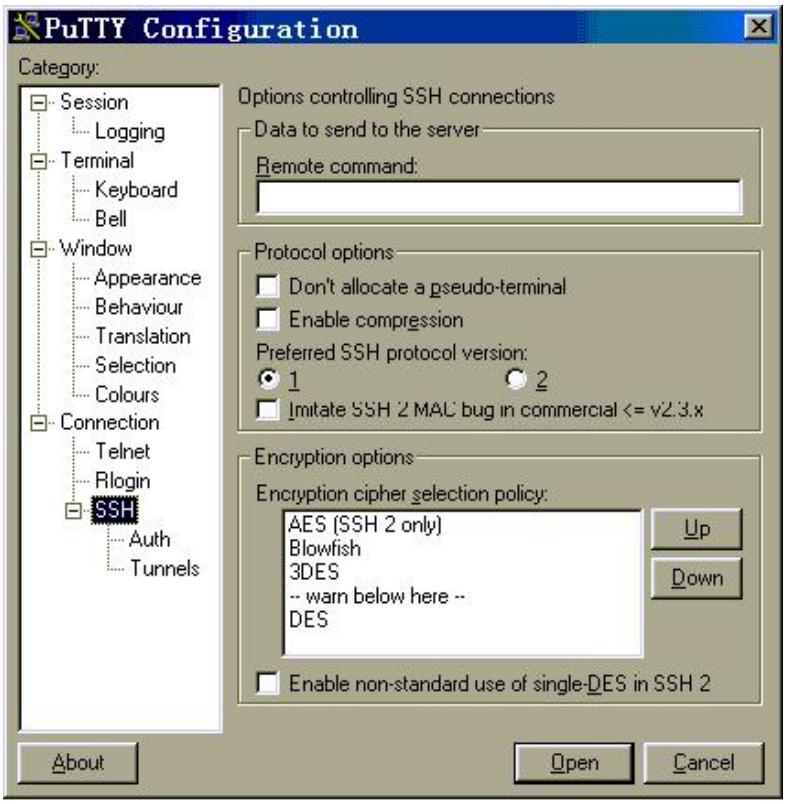


图8-3 SSH 客户端配置界面（2）

指定 SSH 版本为“1”，如上图。

4. 指定 RSA 私钥文件

如果用户需要 RSA 认证，就必须指定 RSA 私钥文件。如果用户只需要密码认证，则不需要指定 RSA 私钥文件。

如上图，单击“SSH”下面的“Auth”（认证），出现如下界面：

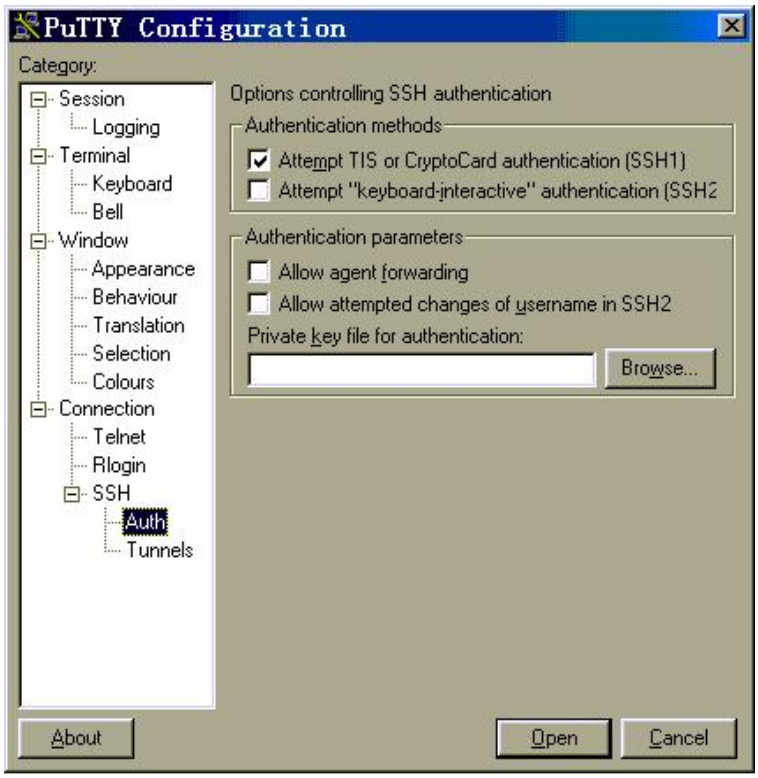


图8-4 SSH 客户端配置界面（3）

单击[Browse]按钮，弹出文件选择窗口。选择私钥文件，并确定即可。

5. 以口令方式打开 SSH 连接

单击[Open]按钮，出现 SSH 客户端界面，如果连接正常则会提示用户输入用户名及口令，如下图：

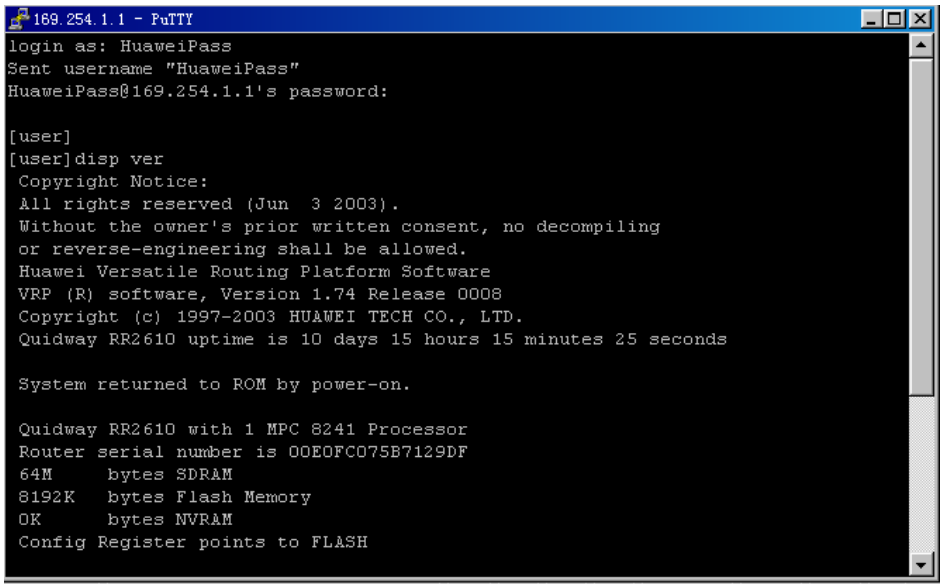


图8-5 SSH 客户端界面

(1) 输入正确的用户名和口令，即可成功进行 SSH 登录连接。

(2) 退出登录，请执行 logout 命令即可。

8.1.4 SSH 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 SSH 的运行情况，通过查看显示信息认证配置的效果。

在用户视图下，执行 **debugging** 命令可对 SSH 进行调试。

SSH 的显示和调试，就是查看各个 SSH 用户的配置情况，更好的利用系统资源，实现安全的信息连接。

请在所有视图下进行下列操作。

表8-10 查看 SSH 相关信息

操作	命令
查看主机和服务器密钥对的公钥部分	**display rsa local-key-pair public**
显示客户端的 RSA 公共密钥	**display rsa peer-public-key** [**brief** | **name** *keyname*]
显示 SSH 状态信息和会话信息	**display ssh server** { **status** | **session** }
显示 SSH 用户信息	**display ssh user-information** [*username*]
打开 SSH 调试开关	**debugging ssh server** { **VTY** *index* | **all** }
关闭 SSH 调试开关	**undo debugging ssh server** { **VTY** *index* | **all** }

8.1.5 SSH 配置举例

1. 组网需求

如 图 8-6，配置终端（SSH Client）与以太网交换机建立本地连接。终端采用SSH协议进行登录到交换机上，以保证数据信息交换的安全。

2. 组网图

图8-6 SSH 本地配置组网图

3. 配置步骤

以下将根据登录认证方式的不同分别介绍配置步骤，但开始任何一种配置之前，首先要执行如下操作：

[Quidway] rsa local-key-pair create

📖 说明：

如果此前已完成生成本地密钥对的配置，可以略过此项操作。

- SSH 认证方式为口令认证。

[Quidway] user-interface vty 0 4

[Quidway-ui-vty0-4] authentication-mode scheme

[Quidway-ui-vty0-4] protocol inbound ssh

[Quidway] local-user client001

[Quidway-luser-client001] password simple huawei

[Quidway-luser-client001] service-type ssh

[Quidway] ssh user client001 authentication-type password

SSH 的认证超时时间、重试次数以及服务器密钥更新时间可以采取系统默认值，这些配置完成以后，您就可以在其它与以太网交换机连接的终端上，运行支持 SSH1.5 的客户端软件，以用户名 client001，密码 huawei，访问以太网交换机了。

- SSH 认证方式为 RSA。

创建本地用户 client002

[Quidway] local-user client002

[Quidway-luser-client002] service-type ssh

设置用户接口上认证模式为 AAA 认证

[Quidway] user-interface vty 0 4

[Quidway-ui-vty0-4] authentication-mode sheme

设置交换机上远程用户登录协议为 SSH。

[Quidway-ui-vty0-4] protocol inbound ssh

#设置交换机上远程用户的认证方式为 RSA。

[Quidway] ssh user client002 authentication-type RSA

#设置交换机上 RSA 的密钥对。

[Quidway] rsa peer-public-key quidway002

[Quidway-rsa-public] public-key-code begin

[Quidway-key-code]
308186028180739A291ABDA704F5D93DC8FDF84C427463

[Quidway-key-code]
1991C164B0DF178C55FA833591C7D47D5381D09CE82913

[Quidway-key-code]
D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4

[Quidway-key-code]
0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC

[Quidway-key-code]
C48E3306367FE187BDD944018B3B69F3CBB0A573202C16

[Quidway-key-code]
BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125

[Quidway-key-code] public-key-code end

[Quidway-rsa-public] peer-public-key end

[Quidway] ssh user client002 assign rsa-key key002

📖 **说明：**

在客户端，需要为该 SSH 用户 client002 指定与 RSA 公钥对应的 RSA 私钥。

这时您可以在保留有 RSA 私钥的终端上运行支持 SSH1.5 的客户端软件，进行相应的配置，即可建立 SSH 连接了。

目　录

第1章 Quidway 系列以太网交换机简介

1.1 Quidway 系列以太网交换机简介

华为推出全系列、全线速的 Quidway 系列以太网交换机，覆盖了从低端到高端、从接入到核心所有领域，提供丰富的二层、三层特性和统一的网管，满足客户对网络的各种要求。华为 Quidway 系列以太网交换机组网方式灵活，既可以应用于企业网络，也可以用于运营商的宽带网络。

📖 **说明：**

关于交换机提供的特性，可以参见相应产品的用户手册。

1.1.1 低端以太网交换机

华为低端系列以太网交换机主要位于网络的接入层，包括 S2008B、S2016B、S2026B、S2000 系列（S2008、S2016、S2026、S2403H）、S3000 系列（S3026、S3026 FM、S3026 FS、S3026E、S3026E FM、S3026E FS）、S2000-SI/S3000-SI 系列（S2026C-SI、S202Z-SI、S3026C-SI、S3026G-SI、S3026S-SI）、S3000-EI 系列（S3026C-EI、S3026G-EI、S3026T-EI）、S3500 系列（S3526、S3526 FM、S3526 FS、S3526E、S3526E FM、S3526E FS、S3526C、S3552）、S5000 系列。其中 S3500 系列具有三层功能，是二/三层以太网交换机，其它交换机都是二层交换机。

1.1.2 中端以太网交换机

华为中端系列以太网交换机主要位于网络的汇聚层，包括 S5516、S6500 系列二/三层以太网交换机。

1.1.3 高端以太网交换机

华为高端以太网交换机位于网络的核心层，包括 S8016 路由交换机、S8500 系列路由交换机等。

1.2 本模块简介

华为 Quidway 系列以太网交换机组网方式灵活，既可以应用于企业网络，也可以用于宽带接入，本模块主要介绍中低端以太网交换机的几种典型组网案例，包括宽带小区网、中小企业网。

第2章 宽带小区网络

2.1 组网需求

宽带小区的组网，要求可认证、可计费、可授权，同时可以进行集中管理，达到电信级的可运营、可管理的要求。

2.2 使用 CAMS 构造宽带小区网络

2.2.1 解决方案

在宽带小区以太网接入中，S3026 以太网交换机放在小区楼道，下行直接接入用户或者通过 S2000 系列以太网交换机接入用户，向上可以通过 GE、FE 连接到小区中心设备（如 S3526 以太网交换机），S3526 通过一个 L3（如 S8016 等）接入到城域网。

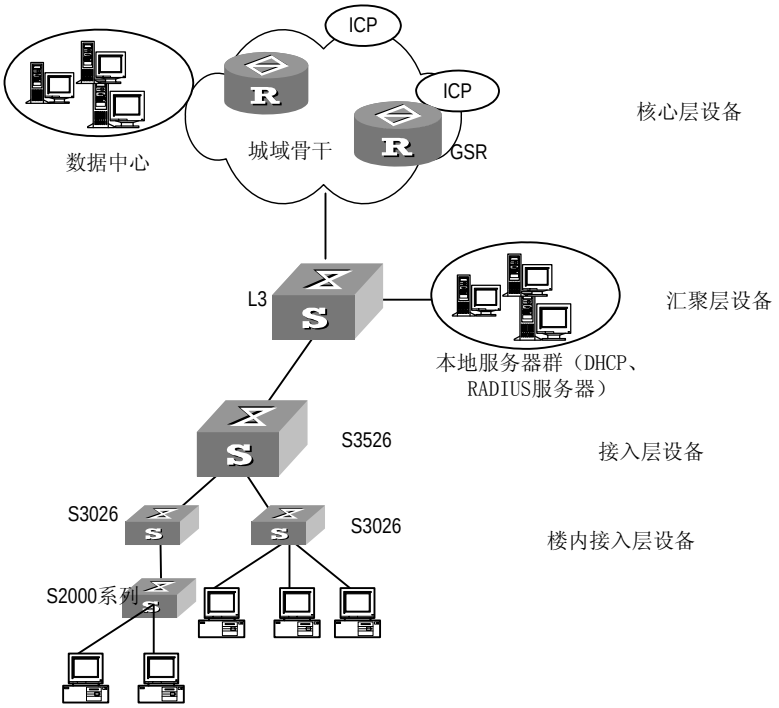


图2-1 小区以太网接入组网示意图

在组网中为了对每个用户进行认证、授权和计费，需要配置 802.1x；同时需要将每个用户进行二层隔离；为了便于网管，需要配置 SNMP；为了防止交换机被非法访问，交换机上需要配置对访问方式的 ACL 控制。

整个网络采用 VLAN10 作为管理 VLAN，所有交换机上 VLAN10 接口的 IP 地址在同一个网段 10.110.110.0/24，主 RADIUS 服务器的 IP 为 10.110.10.18；网管工作站的 IP 地址为 10.11.10.1。

在 S3026 上作如下配置：isolate-user-vlan 配置，将小区每个用户之间进行二层隔离，每个用户分配在一个 Secondary VLAN 内；802.1x 认证配置，认证方式为通过 RADIUS 服务器对用户进行认证；管理 VLAN 配置、网管路由配置、SNMP 配置、各种访问方式的 ACL 控制配置；hybrid 端口配置。

在 S3526 上进行如下配置：网关配置、hybrid 端口配置、SNMP 配置、各种访问方式的 ACL 控制配置。

2.2.2 配置步骤

这里简单说明交换机上的基本配置。

📖 **说明：**

本文仅说明交换机上的基本配置。CAMS 可以在网络运行过程中对交换机进行维护和管理。关于 CAMS 如何对交换机进行配置请参见 CAMS 的用户手册，这里就不再说明。

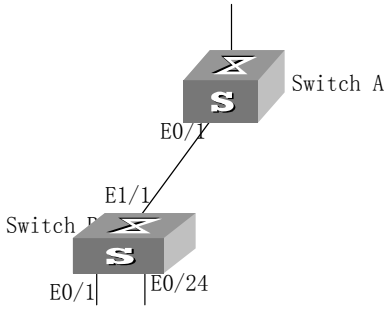


图2-2 组网示意图

1. 配置 Switch B

下面以网络中某台 Switch B 为例说明基本配置过程。

配置 Switch B：配置 isolate-user-vlan（isolate-user-vlan 为 VLAN5）、进行管理 VLAN 配置（配置管理 VLAN 的 IP 地址、一条路由）、配置 802.1x 认证、配置访问方式的 ACL 控制。管理 VLAN10 的 IP 地址为 10.110.110.2，网管站的 IP 地址为 10.11.10.1，向网管站发送数据的下一跳为 10.110.110.1。

(1)　配置 isolate-user-vlan。

配置 isolate-user-vlan。

[Quidway] vlan 5

[Quidway-vlan5] isolate-user-vlan enable

[Quidway-vlan5] port ethernet 1/1

配置 Secondary VLAN。

[Quidway] vlan 2

[Quidway-vlan2] port ethernet 0/1

[Quidway-vlan2] quit

[Quidway] vlan 3

[Quidway-vlan3] port ethernet 0/2

[Quidway-vlan3] quit

依此类推。

[Quidway] vlan 25

[Quidway-vlan25] port ethernet 0/24

[Quidway-vlan25] quit

配置 isolate-user-vlan 和 Secondary VLAN 间的映射关系。

[Quidway] isolate-user-vlan 5 secondary 2 to 25

(2)　配置管理 VLAN 及路由

管理 VLAN 为 VLAN 10，配置其接口 IP 地址。

[Quidway] vlan 10

[Quidway-vlan10] quit

[Quidway] interface vlan 10

[Quidway-Vlan-interface10] ip address 10.110.110.2 255.255.255.0

配置路由，下一跳为 10.110.110.1。

[Quidway] ip route 10.11.10.1 255.255.255.248 10.110.110.1

(3)　配置 802.1x 认证

端口和设备上启动 802.1x 认证。

[Quidway] dot1x

[Quidway] dot1x interface ethernet 0/1 to ethernet 0/24

配置 802.1x 认证基于 MAC 地址。

[Quidway] dot1x port-method macbased interface ethernet 0/1 to ethernet 0/24

[Quidway] dot1x dhcp-launch

📖 **说明：**

缺省情况下，802.1x 采用的认证方式就是基于 MAC 的认证方式，用户可以不用进行此项配置。

配置到 RADIUS 上进行 AAA 认证。

[Quidway] aaa authentication-scheme auth radius

配置计费失败后仍然允许用户在线。

[Quidway] aaa accounting-scheme acct1 enable online

配置 ISP 域及其属性，如计费方法、认证方法等。

[Quidway] domain risp

[Quidway-isp-risp] authen-scheme auth

[Quidway-isp-risp] acct-scheme acct1

[Quidway-isp-risp] state active

[Quidway-isp-risp] radius-scheme hostrmt

配置 RADIUS 属性（主 RADIUS 服务器的 IP 为 10.110.10.18）。

[Quidway] radius scheme hostrmt

[Quidway-radius-hostrmt] primary authentication 10.110.10.18

[Quidway-radius-hostrmt] primary accounting 10.110.10.18

[Quidway-radius-hostrmt] key authentication huawei

[Quidway-radius-hostrmt] key accounting huawei

(4)　配置上行端口 Ethernet1/1 为 hybrid 端口

配置该端口为 hybrid 端口，允许 VLAN5 和 VLAN10 的报文通过。

[Quidway] interface Ethernet1/1

[Quidway-Ethernet1/1] port link-type hybrid

[Quidway-Ethernet1/1] port hybrid pvid vlan 5

[Quidway-Ethernet1/1] port hybrid vlan 10 tagged

(5)　配置 SNMP

进入全局配置模式。

<Quidway> system-view

设置团体名和访问权限。

[Quidway] snmp-agent community read huawei

[Quidway] snmp-agent community write beiyan

设置管理员标识、联系方法以及以太网交换机的物理位置。

[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306

[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor

允许发送 Trap。

[Quidway] snmp-agent trap enable

定义访问控制列表。

[Quidway] acl number 1

[Quidway-acl-basic-1] rule 0 permit source 10.11.10.1 0

创建 SNMP 组，并定义访问控制。

[Quidway] snmp-agent group v3 huaweigroup acl 1

为 SNMP 组添加一个用户 huaweimanager，设置认证密码为 hello，并配置访问控制，只允许网管工作站访问交换机。

[Quidway] snmp-agent usm-user v3 huaweimanager huaweigroup auth md5 huawei acl 1

(6)　配置对 TELNET 用户的访问控制，仅允许 IP 为 10.110.110.46 和 10.110.110.52 的用户通过 TELNET 访问交换机。

定义基本访问控制列表。

[Quidway] acl number 20

[Quidway-acl-basic-20] rule 0 permit source 10.110.110.46 0

[Quidway-acl-basic-20] rule 1 permit source 10.110.110.52 0

引用访问控制列表。

[Quidway] user-interface vty 0 4

[Quidway-ui-vty0-4] acl 20 inbound

(7)　配置对 HTTP 用户的访问控制，仅允许 IP 地址为 10.110.110.46 的主机通过 WEB 方式访问交换机。

定义基本访问控制列表。

[Quidway] acl number 30

[Quidway-acl-basic-30] rule 0 permit source 10.110.110.46 0

引用访问控制列表。

[Quidway] ip http acl 30

2. 配置 Switch A

下面以一台 Switch A 为例介绍配置。

(1)　配置 Ethernet0/1 为 hybrid 端口。

配置 Switch A 的端口 Ethernet0/1 为 hybrid 端口，并允许 VLAN1 和 VLAN5 的报文通过。

[Quidway] interface Ethernet0/1

[Quidway-Ethernet0/1] port link-type hybrid

[Quidway-Ethernet0/1] port hybrid pvid vlan 5

[Quidway-Ethernet0/1] port hybrid vlan 1 tagged

(2)　配置 VLAN5 的接口 IP 地址

创建 VLAN5。

[Quidway] vlan 5

配置 VLAN5 的接口 IP 地址。

[Quidway] interface vlan 5

[Quidway-Vlan-interface5] ip address 10.110.11.1 255.255.255.192

创建 VLAN10。

[Quidway] vlan 10

配置 VLAN10 的接口 IP 地址。

[Quidway] interface vlan 10

[Quidway-Vlan-interface10] ip address 10.110.110.1 255.255.255.0

(3)　配置 SNMP

进入全局配置模式。

<Quidway> system-view

设置团体名和访问权限。

[Quidway] snmp-agent community read huawei

[Quidway] snmp-agent community write beiyan

设置管理员标识、联系方法以及以太网交换机的物理位置。

[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306

[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor

允许发送 Trap。

[Quidway] snmp-agent trap enable

定义访问控制列表，以便进行对通过 SNMP 登录交换机的用户进行 ACL 控制。

[Quidway] acl number 1

[Quidway-acl-basic-1] rule 0 permit source 10.11.10.1 0

创建 SNMP 组，并定义访问控制。

[Quidway] snmp-agent group v3 huaweigroup acl 1

为 SNMP 组添加一个用户 huaweimanager，设置认证密码为 hello，并配置访问控制，只允许网管工作站访问交换机。

[Quidway] snmp-agent usm-user v3 huaweimanager huaweigroup auth md5 huawei acl 1

(4) 配置对 TELNET 用户的访问控制，仅允许 IP 为 10.110.110.46 和 10.110.110.52 的用户通过 TELNET 访问交换机。

定义基本访问控制列表。

[Quidway] acl number 20

[Quidway-acl-basic-20] rule 0 permit source 10.110.110.46 0

[Quidway-acl-basic-20] rule 1 permit source 10.110.110.52 0

引用访问控制列表。

[Quidway] user-interface vty 0 4

[Quidway-ui-vty0-4] acl 20 inbound

(5) 配置对 HTTP 用户的访问控制，仅允许 IP 地址为 10.110.110.46 的主机通过 WEB 方式访问交换机。

定义基本访问控制列表。

[Quidway] acl number 30

[Quidway-acl-basic-30] rule 0 permit source 10.110.110.46 0

引用访问控制列表。

[Quidway] ip http acl 30

📖 **说明：**

Switch A 可能下挂很多 Switch B，需要配置多个 VLAN 和 VLAN 接口 IP 地址。本例仅以配置 VLAN5 为例。

在实际组网中一般采用 S2000 系列（如 S2008、S2016、S2403H）接入用户。

2.3 利用 MA5200 构造宽带小区网络

2.3.1 解决方案

在宽带城域网组网图中，S3026 以太网交换机作为宽带城域网的小区接入层交换机，通过与管理设备 MA5200 的配合实现宽带接入服务，两者之间的通信可通过 HGMP（Huawei Group Management Protocol）来承载。通过 S3026 的 HGMP 代理程序，管理设备 MA5200 可以实现对 S3026 的集中管理。MA5200 可以通过上行高速口直接连接到城域网或骨干网，多台 S3026 上行

直接挂在 MA5200 的 100Mbit/s 以太网光接口上，下行接到小区用户的计算机上。

“MA5200”加“S3026”的组网具备了用户管理、认证、鉴权和按时按量计费等多方面的的优势，使之既有以太网接入经济、成熟的特色，又有电信级的用户管理和运营能力，适用于新建小区和商用大楼，也可以运用于商业网的宽带化。

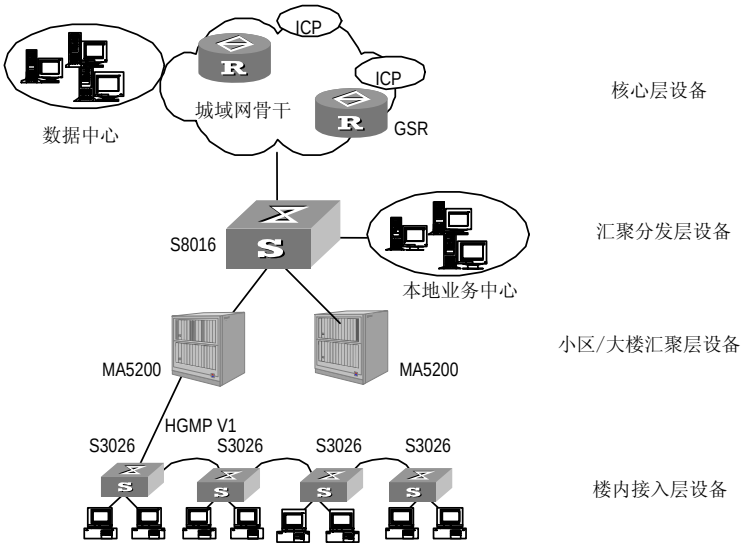


图2-3 宽带接入组网示意图

2.3.2 配置步骤

MA5200 的配置可以参见 MA5200 的用户手册，这里不再说明。S3026 除了进行一些基本配置以外，还需要启动 HGMP Client，以实现集中管理特性。

📖 说明：

S3026 以太网交换机作为 HGMP Client 时，必须要通过固定的上行端口与管理设备相连。这些上行端口为：Ethernet0/24、Ethernet1/1、Ethernet2/1。

---

1. 配置 S3026

下面以网络中某台 S3026 为例说明基本配置过程。

配置一台 S3026：进行管理 VLAN 配置、配置 802.1x 认证、配置访问方式的 ACL 控制。管理 VLAN10 的 IP 地址为 10.110.110.2，网管站的 IP 地址为 10.11.10.1。

(1) 配置 VLAN。

[Quidway] vlan 2

[Quidway-vlan2] port ethernet 0/1

[Quidway-vlan2] quit

[Quidway] vlan 3

[Quidway-vlan3] port ethernet 0/2

[Quidway-vlan3] quit

依此类推。

[Quidway] vlan 25

[Quidway-vlan25] port ethernet 0/24

[Quidway-vlan25] quit

(2) 配置管理 VLAN 及路由

管理 VLAN 为 VLAN 10，配置其接口 IP 地址。

[Quidway] vlan 10

[Quidway-vlan10] quit

[Quidway] interface vlan 10

[Quidway-Vlan-interface10] ip address 10.110.110.2 255.255.255.0

配置路由，下一跳为 10.110.110.1。

[Quidway] ip route 10.11.10.1 255.255.255.248 10.110.110.1

(3) 配置 802.1x 认证

端口和设备上启动 802.1x 认证。

[Quidway] dot1x

[Quidway] dot1x interface ethernet 0/1 to ethernet 0/24

配置 802.1x 认证基于 MAC 地址。

[Quidway] dot1x port-method macbased interface ethernet 0/1 to ethernet 0/24

[Quidway] dot1x dhcp-launch

📖 **说明：**

缺省情况下，802.1x 采用的认证方式就是基于 MAC 的认证方式，用户可以不用进行此项配置。

配置到 RADIUS 上进行 AAA 认证。

[Quidway] aaa authentication-scheme auth radius

配置计费失败后仍然允许用户在线。

[Quidway] aaa accounting-scheme acct1 enable online

配置 ISP 域及其属性，如计费方法、认证方法等。

[Quidway] domain risp

[Quidway-isp-risp] authen-scheme auth

[Quidway-isp-risp] acct-scheme acct1

[Quidway-isp-risp] state active

[Quidway-isp-risp] radius-scheme hostrmt

配置 RADIUS 属性（主 RADIUS 服务器的 IP 为 10.110.10.18）。

[Quidway] radius scheme hostrmt

[Quidway-radius-hostrmt] primary authentication 10.110.10.18

[Quidway-radius-hostrmt] primary accounting 10.110.10.18

[Quidway-radius-hostrmt] key authentication huawei

[Quidway-radius-hostrmt] key accounting huawei

(4)　配置上行端口 Ethernet1/1 为 trunk 端口

配置该端口为 trunk 端口，允许所有的报文通过。

[Quidway] interface Ethernet1/1

[Quidway-Ethernet1/1] port link-type trunk

[Quidway-Ethernet1/1] port trunk pvid vlan 5

[Quidway-Ethernet1/1] port trunk permit vlan all

(5)　配置 SNMP

进入全局配置模式。

<Quidway> system-view

设置团体名和访问权限。

[Quidway] snmp-agent community read huawei

[Quidway] snmp-agent community write beiyan

设置管理员标识、联系方法以及以太网交换机的物理位置。

[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306

[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor

允许发送 Trap。

[Quidway] snmp-agent trap enable

定义访问控制列表。

[Quidway] acl number 1

[Quidway-acl-basic-1] rule 0 permit source 10.11.10.1 0

创建 SNMP 组，并定义访问控制。

[Quidway] snmp-agent group v3 huaweigroup acl 1

为 SNMP 组添加一个用户 huaweimanager，设置认证密码为 hello，并配置访问控制，只允许网管工作站访问交换机。

[Quidway] snmp-agent usm-user v3 huaweimanager huaweigroup auth md5 huawei acl 1

(6) 配置对 TELNET 用户的访问控制，仅允许 IP 为 10.110.110.46 和 10.110.110.52 的用户通过 TELNET 访问交换机。

定义基本访问控制列表。

[Quidway] acl number 20

[Quidway-acl-basic-20] rule 0 permit source 10.110.110.46 0

[Quidway-acl-basic-20] rule 1 permit source 10.110.110.52 0

引用访问控制列表。

[Quidway] user-interface vty 0 4

[Quidway-ui-vty0-4] acl 20 inbound

(7) 配置对 HTTP 用户的访问控制，仅允许 IP 地址为 10.110.110.46 的主机通过 WEB 方式访问交换机。

定义基本访问控制列表。

[Quidway] acl number 30

[Quidway-acl-basic-30] rule 0 permit source 10.110.110.46 0

引用访问控制列表。

[Quidway] ip http acl 30

启动 HGMP client

通过以下步骤在 S3026 上启动 HGMP Client：

(8) 重新启动交换机

(9) 在以太网交换机启动的时候使用组合键“Ctrl＋B”进入 Bootrom 菜单。

(10) 选择选项“6. Set switch HGMP mode”使交换机选择 HGMP 模式启动。

(11) 系统会提示当前 HGMP 模式是关闭的，并询问是否确认打开 HGMP 模式“Current HGMP mode is OFF. Are you sure to turn on HGMP mode? Yes or No(Y/N)”。

(12) 回答“Y”，则系统提示 HGMP 模式被打开，显示“Turn on HGMP mode successfully!”。此时系统重新进入 Bootrom 主菜单。用户可以选择选项“0. Reboot”来启动以太网交换机。

S3026 上启动了 HGMP Client 后，MA5200 可以作为管理设备对下挂的 S3026 进行集中管理。

第3章 中小企业/大企业分支机构组网

3.1 组网需求

中小企业的组网，没有认证、计费、授权等需求，只要保证内部网络安全、各个部门限制相互访问就可以了。

3.2 利用华为交换机构造企业网络

3.2.1 解决方案

在中小企业或大企业的分支机构中，二层以太网交换机作为二层汇聚交换机，可以直接接用户，上行连接到二/三层以太网交换机，可以通过路由器连接到总部或其它分支机构的网络。

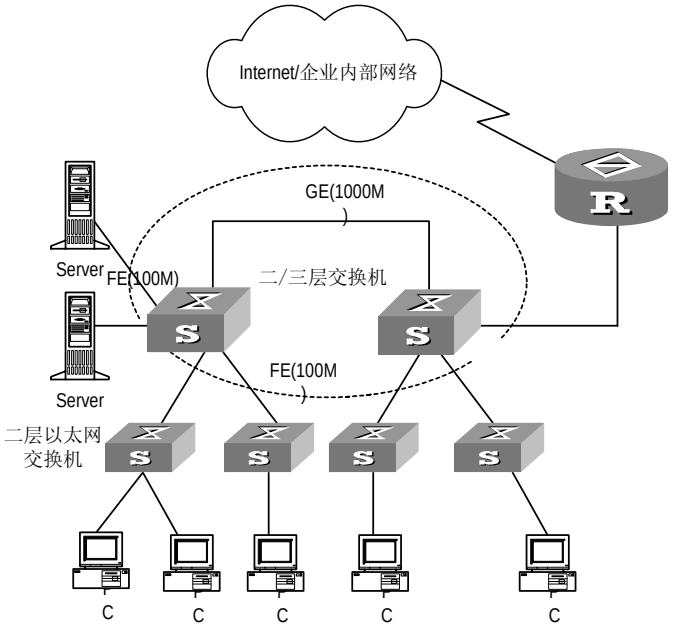


图3-1 中小企业、大企业分支机构组网示意图

在组网中将每个部门划分在一个 VLAN 中；为了便于网管，需要配置 SNMP；为了防止交换机被非法访问，交换机上需要配置对访问方式的 ACL 控制。

整个网络采用 VLAN10 作为管理 VLAN，所有交换机上 VLAN10 接口的 IP 地址在同一个网段 10.110.110.0/24，主 RADIUS 服务器的 IP 为 10.110.10.18；

网管工作站的 IP 地址为 10.11.10.1。路由器的 IP 地址为 10.100.11.1，二/三层交换机通过 VLAN2 接口与路由器相连，VLAN2 接口的 IP 地址为 10.100.11.2。

在二层交换机上作如下配置：管理 VLAN 配置、网管路由配置、SNMP 配置、各种访问方式的 ACL 控制配置；hybrid 端口配置。

在二/三层交换机上进行如下配置：网关配置、hybrid 端口配置、SNMP 配置、各种访问方式的 ACL 控制配置、各个部门间的相互访问的控制。

3.2.2 配置步骤

根据作好的网络规划，对各个交换机进行配置。这里仅简单说明交换机上的配置。

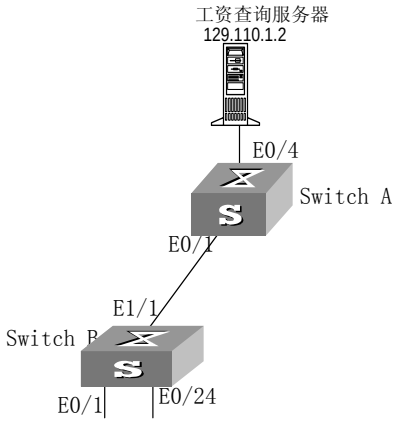


图3-2 S3026 的实际组网情况

1. 配置 Switch B

下面以网络中某部门的 Switch B 为例说明基本配置过程。此部门所有的计算机配置在一个 VLAN 内。

(1)　配置 VLAN。

[Quidway] vlan 5

[Quidway-vlan5] port ethernet 0/1 to Ethernet 0/24 ethernet 1/1

[Quidway-vlan5] quit

(2)　配置管理 VLAN 及路由

管理 VLAN 为 VLAN 10。

[Quidway] interface vlan 10

[Quidway-Vlan-interface10] ip address 10.110.110.2 255.255.255.0

配置路由，下一跳为 10.110.110.1。

[Quidway] ip route 10.11.10.1 255.255.255.248 10.110.110.1

(3) 配置上行端口 Ethernet1/1 为 hybrid 端口，允许 VLAN10 和 VLAN5 的报文通过。

[Quidway] interface Ethernet1/1

[Quidway-Ethernet1/1] port link-type hybrid

[Quidway-Ethernet1/1] port hybrid pvid vlan 5

[Quidway-Ethernet1/1] port hybrid vlan 10 tagged

(4) 配置 SNMP

进入全局配置模式。

<Quidway> system-view

设置团体名和访问权限。

[Quidway] snmp-agent community read huawei

[Quidway] snmp-agent community write beiyan

设置管理员标识、联系方法以及以太网交换机的物理位置。

[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306

[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor

允许发送 Trap。

[Quidway] snmp-agent trap enable

定义访问控制列表，以便进行对通过 SNMP 访问交换机的用户进行 ACL 控制。

[Quidway] acl number 1

[Quidway-acl-basic-1] rule 0 permit source 10.11.10.1 0

创建 SNMP 组，并定义访问控制。

[Quidway] snmp-agent group v3 huaweigroup acl 1

为 SNMP 组添加一个用户 huaweimanager，设置认证密码为 hello，并配置访问控制，只允许网管工作站访问交换机。

[Quidway]snmp-agent usm-user v3 huaweimanager huaweigroup auth md5 huawei acl 1

(5) 配置对 TELNET 用户的访问控制，仅允许 IP 为 10.110.110.46 和 10.110.110.52 的用户通过 TELNET 访问交换机。

定义基本访问控制列表。

[Quidway] acl number 20

[Quidway-acl-basic-20] rule 0 permit source 10.110.110.46 0

[Quidway-acl-basic-20] rule 1 permit source 10.110.110.52 0

引用访问控制列表。

[Quidway] user-interface vty 0 4

[Quidway-ui-vty0-4] acl 20 inbound

(6) 配置对 HTTP 用户的访问控制，仅允许 IP 地址为 10.110.110.46 的主机通过 WEB 方式访问交换机。

定义基本访问控制列表。

[Quidway] acl number 30

[Quidway-acl-basic-30] rule 0 permit source 10.110.110.46 0

引用访问控制列表。

[Quidway] ip http acl 30

2. 配置 Switch A

下面以一台 Switch A 为例介绍配置。

(1) 配置下面接 Switch B 的端口 Ethernet0/1 为 hybrid 端口，并允许 VLAN10 和 VLAN5 的报文通过。

[Quidway] interface Ethernet0/1

[Quidway-Ethernet0/1] port link-type hybrid

[Quidway-Ethernet0/1] port hybrid pvid vlan 5

[Quidway-Ethernet0/1] port hybrid vlan 10 tagged

(2) 配置 VLAN5 的接口 IP 地址

创建 VLAN5。

[Quidway] vlan 5

配置 VLAN5 的接口 IP 地址。

[Quidway] interface vlan 5

[Quidway-Vlan-interface5] ip address 10.110.11.1 255.255.255.192

(3)　配置到 Switch B 管理 VLAN 的静态路由。

配置到 Switch B 管理 VLAN 的静态路由，以便对 Switch B 进行管理。

[Quidway] ip route 10.110.110.2 255.255.255.0 10.110.110.1

(4)　配置到路由器的静态路由。

路由器的 IP 地址为 10.100.11.1，Switch A 通过 VLAN2 接口与路由器相连，VLAN2 接口的 IP 地址为 10.100.11.2。

创建 VLAN2 及其接口，并配置 IP 地址。

[Quidway] vlan 2

[Quidway] interface vlan 2

[Quidway-Vlan-interface2] ip address 10.100.11.2 255.255.255.248

配置到路由器的静态路由。

[Quidway] ip route 10.100.11.1 255.255.255.248 vlan 2

(5)　配置 SNMP

进入全局配置模式。

<Quidway> system-view

设置团体名和访问权限。

[Quidway] snmp-agent community read huawei

[Quidway] snmp-agent community write beiyan

设置管理员标识、联系方法以及以太网交换机的物理位置。

[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306

[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor

允许发送 Trap。

[Quidway] snmp-agent trap enable

定义访问控制列表，以便进行对通过 SNMP 登录交换机的用户进行 ACL 控制。

[Quidway] acl number 1

[Quidway-acl-basic-1] rule 0 permit source 10.11.10.1 0

创建 SNMP 组，并定义访问控制。

[Quidway] snmp-agent group v3 huaweigroup acl 1

为 SNMP 组添加一个用户 huaweimanager，设置认证密码为 hello，并配置访问控制，只允许网管工作站访问交换机。

[Quidway] snmp-agent usm-user v3 huaweimanager huaweigroup auth md5 huawei acl 1

(6) 配置对 TELNET 用户的访问控制，仅允许 IP 为 10.110.110.46 和 10.110.110.52 的用户通过 TELNET 访问交换机。

定义基本访问控制列表。

[Quidway] acl number 20

[Quidway-acl-basic-20] rule 0 permit source 10.110.110.46 0

[Quidway-acl-basic-20] rule 1 permit source 10.110.110.52 0

引用访问控制列表。

[Quidway] user-interface vty 0 4

[Quidway-ui-vty0-4] acl 20 inbound

(7) 配置对 HTTP 用户的访问控制，仅允许 IP 地址为 10.110.110.46 的主机通过 WEB 方式访问交换机。

定义基本访问控制列表。

[Quidway] acl number 30

[Quidway-acl-basic-30] rule 0 permit source 10.110.110.46 0

引用访问控制列表。

[Quidway] ip http acl 30

(8) 配置部门对工资服务器访问的限制，在 8:00～18:00 禁止访问工资服务器。

定义时间段从 8 点到 18 点，命名为 time8to18。

[Quidway] time-range time8to18 from 8:00:00 to 18:00:00

📖 **说明：**

由于交换机自身不带有时钟，所以一旦交换机重启，必须重新设置交换机的时钟上面的时间范围配置才能正确生效。

为 10.110.0.0 网络向工资服务器 129.110.1.2 发送的报文定义一条规则，命名为 Rdeny。

[Quidway] acl name Rdeny advanced

[Quidway-acl-adv-100] rule 0 deny source 10.110.0.0 255.255.192.0 destination 129.110.1.2 255.255.0.0 time-range time8to18

激活或应用 Rdeny。

[Quidway] packet-filter ip-group Rdeny

📖 **说明：**

Switch A 可能下挂很多台 Switch B，需要配置多个 VLAN 和 VLAN 接口 IP 地址。本例仅以配置 VLAN5 为例。

在 Switch A 上也可能需要配置其他一些部门对工资服务器的访问控制，本例仅以其中一个部门为例。

目　录

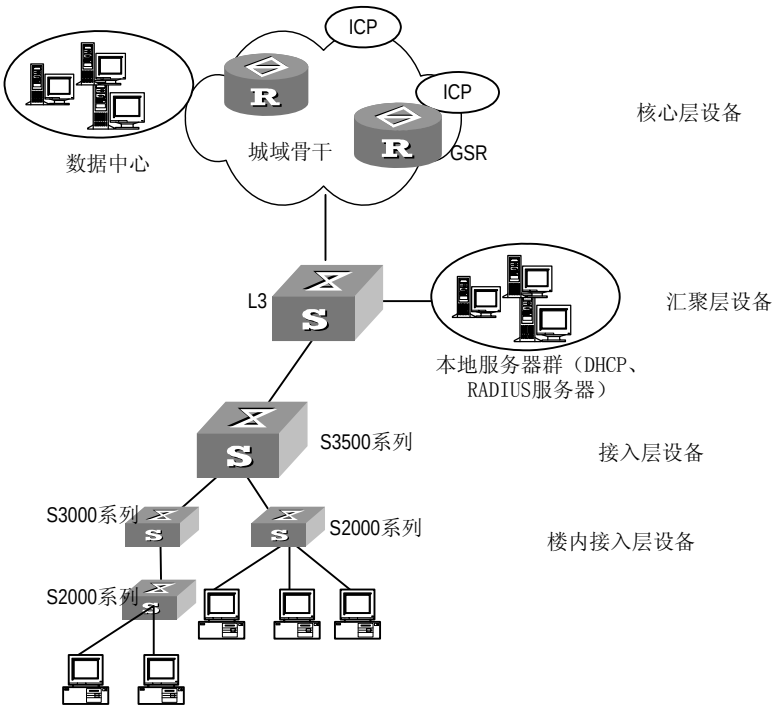
附录 A 交换网络数据转发流程

A.1 引言

随着因特网的高速发展，人们对通信的需求已从传统的电话、传真、电报等低速业务逐渐向高速的因特网接入、可视电话、视频点播等宽带业务领域延伸。用户对上网速率的需求也越来越高，以太网接入因其成本低、使用简单、速度高而倍受市场的关注。面对迅猛发展的宽带网络建设需求，华为公司根据不同的客户类型需求，推出了 Quidway 系列以太网交换机及其它网络设备。使用华为公司的网络设备，可以构建可运营、可管理的网络。那么在网络中，数据是怎样转发的呢？本文将简要讲述数据在交换网络中的转发流程。

A.2 简单的转发流程

下面给出一个简单的组网示意图，以便说明。



图A-1 小区组网示意图

在上图中，L3 表示的是三层交换机，GSR 为 Gigabit Switch Router 的缩写，即 G 比特交换路由器，ICP 为 Internet Content Provider 的缩写，即因特网内容提供商。

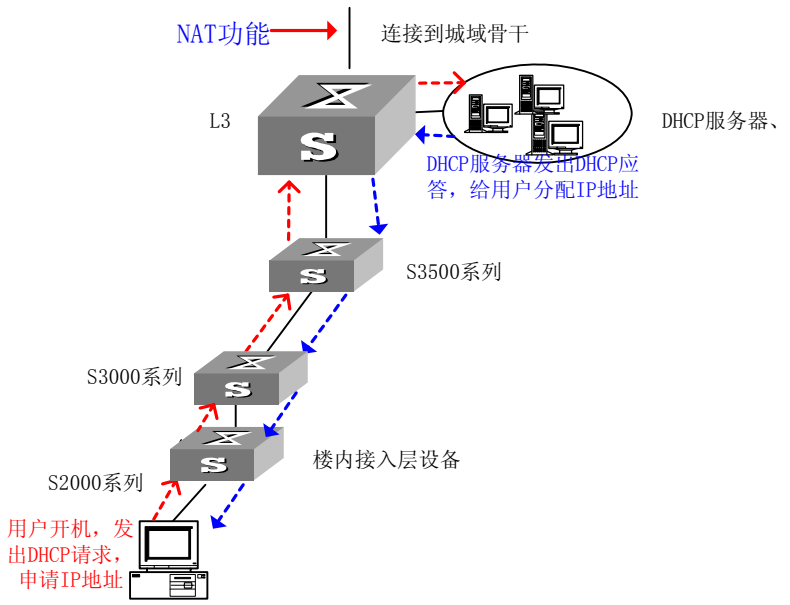
在组网中，接入层设备为华为 S2000 系列和 S3000 系列以太网交换机。汇聚层设备为 S3500 系列以太网交换机或者 S5516、S6506 等三层以太网交换机。小区内部有 AAA（Authentication, Authorization and Accounting）服务器、DHCP（Dynamic Host Configuration Protocol）服务器、DNS（Domain Name Server）服务器。

🕮 **说明：**

实际组网中，用户的计算机可能采用的是固定 IP。用户通过固定 IP 上网与动态申请 IP 上网相比，仅仅是缺少了申请 IP 地址这一过程。所以在下面的例子中，以用户的计算机通过 DHCP 协议动态申请 IP 地址为例进行介绍。
用户计算机配置为自动获取 IP 地址。

下面介绍小区内部数据的转发过程，对数据到达城域网后的过程不作介绍。

用户计算机开机后会通过 DHCP 报文申请 IP 地址。接入层交换机、汇聚层交换机会将此请求报文转发给 DHCP 服务器。DHCP 服务器通过应答报文给用户 PC 分配 IP 地址。有了 IP 地址后，用户就可以上网了。



图A-2 IP 地址请求过程

整个申请 IP 地址的过程如下：

(1) 客户机通过 DHCP Discover 广播提出请求。如果客户机有一个永久性的租用地址，它可以直接请求那个地址。

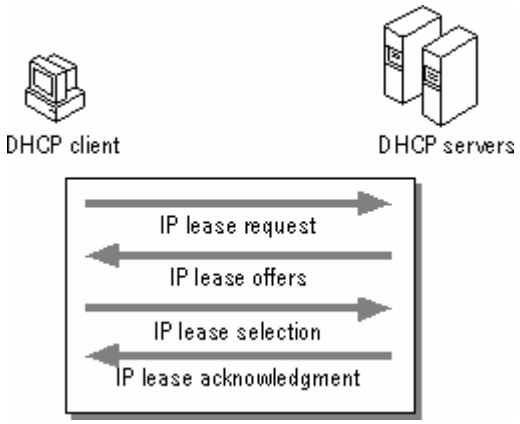
(2) 服务器一旦收到 IP 请求，会从地址池中取出一个地址并返回一个附有可用 IP 地址的 DHCP Offer 报文。

(3) 如果客户机收到多个 IP，它会选择第一个或其所请求的那一个。

(4) 客户机广播标识服务器的 DHCP Request 报文并等待。

(5) 每一个服务器检查报文，若发现不是它的标识，它会丢弃报文。当被标识的服务器接收了报文后，它会发回一个 DHCP Ack 报文，如果所请求的 IP 被分配也就是说租用已中止，会发回 DHCP Nak 报文。

(6) 如果客户机收到 DHCP Ack 报文，它可以开始使用 IP 地址。如果它收到 DHCP Nak，它会重新开始整个过程。假如 IP 有问题，客户机会发送一个 DHCP Decline 报文给服务器并重新开始。



图A-3 IP 地址请求过程示意图

📖 **说明：**

这里有一个问题：如果给每个用户分配的都是公网 IP，会需要大量 IP 地址，这非常浪费，也不现实。所以一般情况下，小区内用户分配的是私网 IP，而在图中的 L3 上实现 NAT 功能。

A.2.1 同一 VLAN 内的通信

用户计算机通过 ARP 在本 PC 上建立一个 IP 与 MAC 地址的对应表格（通往 VLAN 外部的 IP 地址将对应为 VLAN 网关的 IP 地址）。这个表称为 ARP 表。同时 ARP 在存储器中维护一个 cache，这个 cache 称为 ARP cache。通常用户计算机要向外发送报文的时候（进行通信的应用程序不知道对端的物理地址），有如下步骤：

(1) 首先搜索 ARP cache 对目的 IP 进行匹配，如果匹配成功，ARP 就反馈 IP 地址对应的 MAC 地址给进行通信的应用程序；假如没有匹配成功就检查 ARP 表，如果匹配成功，ARP 就反馈 IP 地址对应的 MAC 地址给进行通信的应用程序。

(2) 假如 ARP 没找到一个匹配的 IP 地址，它就会向网络上发布消息，这个消息被称为 ARP 请求。ARP 请求被广播到局域网上的每一个设备。

(3) 如果局域内存在目的 IP 对应的设备，则此设备会向发起 ARP 请求的计算机反馈应答，将自己的 MAC 地址反馈给用户计算机。如果局域网内不存在目的 IP 对应的设备，则网关会将自己的 MAC 地址反馈给用户计算机。

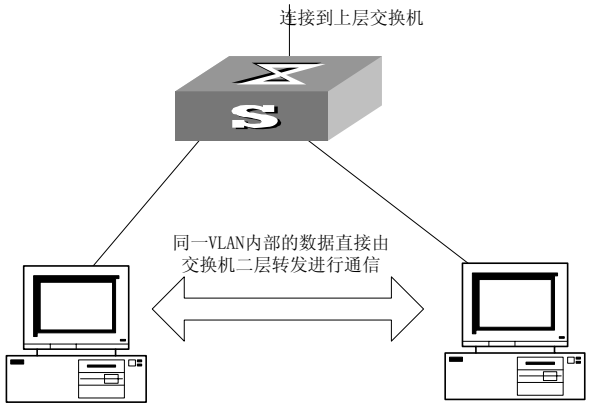
(4) 用户计算机上进行通信的应用程序根据找到的 MAC 地址封装报文，并发送出去。同时用户计算机上的 ARP 会将新找到的 MAC 地址和其对应的 IP 地址作为一个表项添加到 ARP 表和 ARP cache 中。

(5) 交换机收到用户计算机的报文，进行判断，如果通信的源端和目的端在同一个 VLAN 内部，进行二层转发；如果二者不在同一个 VLAN 内，就交给网关进行三层转发。

如果用户在同一个 VLAN 内部通信，只需要进行二层的点到点通信。

📖 **说明：**

VLAN 是虚拟局域网，是将有相同需求的网络设备从逻辑上划分在一个局域网内，而不是按照物理位置划分局域网。VLAN 的详细描述可以参见 IEEE 802.1Q 协议和操作手册中 VLAN 模块。



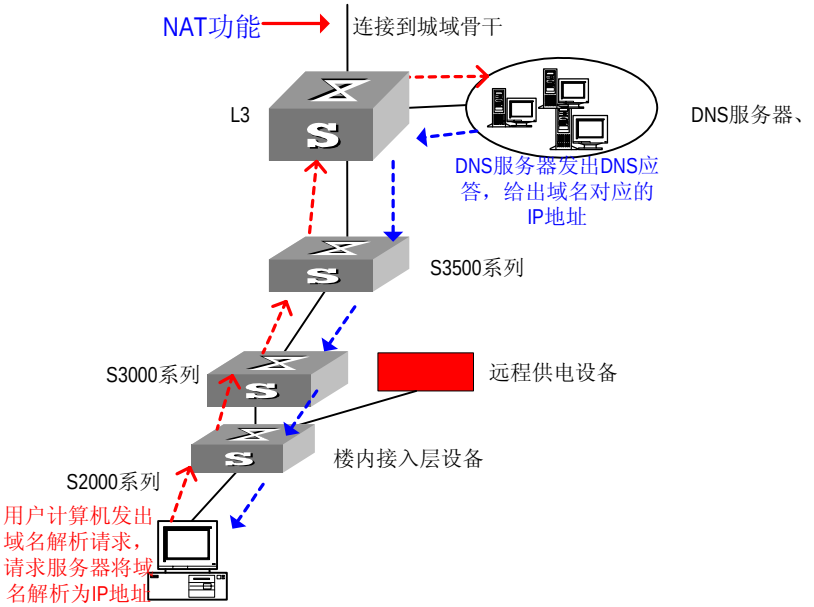
图A-4 同一 VLAN 内的通信示意图

A.2.2 不同 VLAN 间的通信

交换网络中如果没有配置 PVLAN，则不同 VLAN 间的计算机进行通信需要经过路由来实现，这里就不再详细介绍。

A.2.3 用户登录因特网的数据流程

如果用户想要上网，则需要将报文发送给网关；网关再进行三层的路由转发。一般用户会使用域名来访问因特网，这时在登录到指定的网站之前有一个域名解析的过程：用户键入域名后，计算机会向小区内的域名服务器发送一个 DNS 请求报文，小区内的域名服务器会向用户返回域名对应的 IP 地址（用户的计算机上需要正确配置域名服务器的 IP 地址）。



图A-5 域名解析的过程

📖 **说明：**

当小区网络内无 DNS 服务器，而使用小区网络外面的 DNS 服务器时，就会出现内部用户不能通过域名访问 DNS 服务器的情况。原因是：内部 PC 通过域名访问网络时，会到外部的 DNS 上请求 IP 地址，由于 DNS 是在外部，所以它会返回一个公网的地址或找不到地址。这样导致内部 PC 通过域名访问时，得到是外部的地址或者得不到地址，导致小区内部用户不能正常访问小区内部的服务器。

📖 **说明：**

Quidway S2008B、S2016B 以太网交换机支持远程馈电。对这些设备进行远程馈电需要专门的供电设备，同时必须通过指定的交换机端口才能实现远程馈电。一般情况下，供电设备设置在小区的机房中，对小区内所有的需要远程馈电的交换机进行供电。

用户计算机在取得了域名对应的 IP 地址后，就可以访问因特网：

(1) 用户计算机以域名对应的 IP 地址为目的地址，自己的 IP 地址为源 IP 地址封装用户的 TCP 或者 UDP 数据，向网关发送此 IP 数据包；

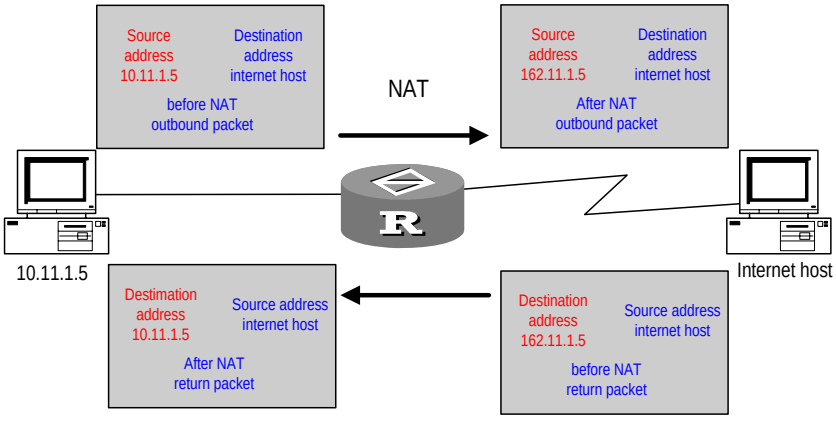
(2) 网关交换机收到此数据后根据路由表将此数据交给图中的 L3 设备；

(3) L3 设备对此数据进行一次 NAT 转换，将源地址改为 L3 的地址池中的一个公网 IP 地址，然后将此数据发送到城域网上；

(4) 当 L3 收到从城域网返回的数据后，进行一次 NAT 操作，将目的 IP 地址转换为相应的私网 IP 地址，然后转发给下挂的相应的交换机；数据沿交换机一层层下发，直到发给用户计算机。

📖 **说明：**

NAT（Network Address Translation），实现私网 IP 地址和公网 IP 地址之间的转换。详细内容可以参见 L3 设备配置指导手册的相关描述或其它技术文档。目前华为的 S8016 交换机实现了 NAT 功能。



图A-6 NAT 的地址转换过程

通过对交换机作简单的配置，小区内的用户就可以上网了。但是，怎样对用户进行计费、认证、授权等操作呢？这就需要构造一个可运营、可管理的交换网络。下面就讲述一下可运营、可管理的网络中的数据转发流程。

A.3 可运营、可管理网络中的数据转发流程

华为 Quidway 系列以太网交换机提供多种特性，可以为运营商构造可运营、可管理的网络。

在用户启动计算机准备上网时，需要首先通过认证，然后才能获取 IP 地址，进行后续的上网过程。

1. 用户的 802.1x 认证过程

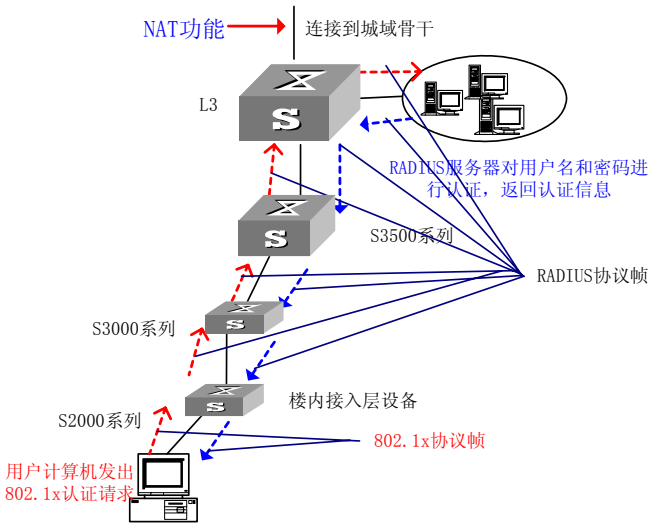
华为 Quidway 系列以太网交换机提供 802.1x 特性，可以对用户进行 802.1x 认证。

计算机上网必须先进行认证：在本计算机上启动 802.1x 终端软件，输入用户名和密码；交换机在收到用户名和密码后有两种认证方式，可以在本地进行认证，也可以通过 RADIUS 服务器进行远端认证。

本地认证需要在交换机上配置相应的用户名和密码，这种方法数据交互流程比较简单，但管理起来比较麻烦，需要在交换机上作很多配置，在组网中一般不会用到。下面就介绍通过 RADIUS 服务器进行认证的数据交互过程。

交换机上首先需要启动 802.1x 认证，并作了相应的配置。配置过程可以参见交换机用户手册的“AAA 及安全协议配置”模块。

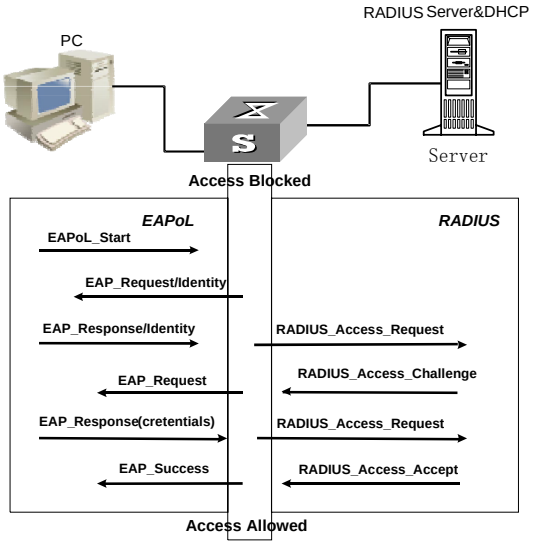
一般情况下交换机和 RADIUS 认证服务器之间传输的是标准的 RADIUS 报文，下面介绍在这种情况下 802.1x 认证的数据交互过程。



图A-7 802.1x 认证数据转发过程

用户计算机使用 802.1x 协议帧封装认证信息，和与之相连的交换机进行交互。交换机则使用标准的 RADIUS 协议封装用户认证信息，这样该认证数据就可

以穿越复杂的网络到达 RADIUS 服务器进行认证。下图为认证的数据交互示意图。其中 EAPoL（EAPOL 是 Extensible Authentication Protocol over LAN 的缩写）数据构成 802.1x 协议帧，RADIUS 数据构成 RADIUS 协议帧。



图A-8 802.1x 认证数据交互过程

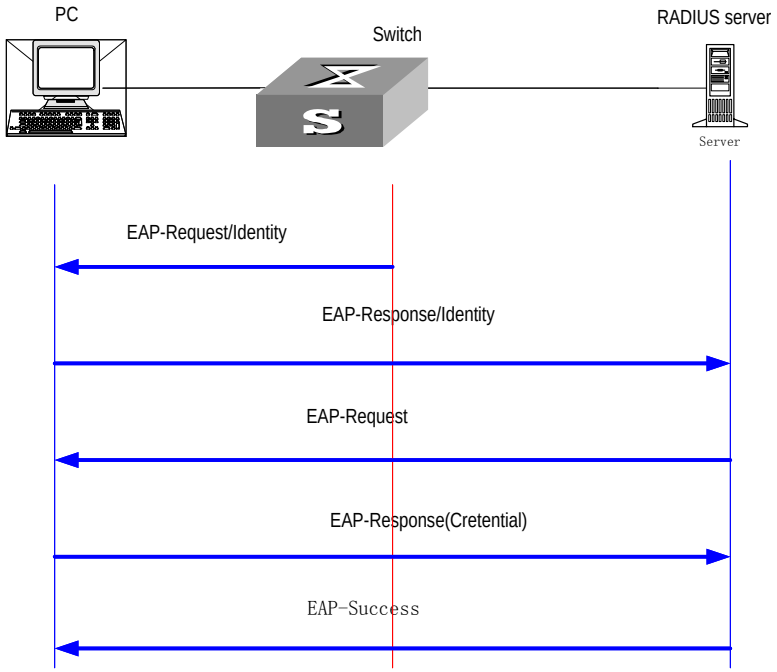
交换机也可以透明传输 802.1x 的 EAP 报文给 RADIUS 服务器。下面介绍这种情况下的 802.1x 认证的数据交互过程。

在这种情况下，从认证客户端到认证服务器直接传递的都是 802.1x 的 EAP 报文。首先交换机和认证客户端之间会进行 EAP 的协商，在协商完成后，会进行 802.1x 认证过程。

📖 **说明：**

在交换机上作了相应的配置之后，交换机就可以透明传输 802.1x 的 EAP 报文。相应的配置信息请参见交换机用户手册配置指导分册的“AAA 及安全协议配置”模块。

802.1x 认证的数据交互过程如下图所示。



图A-9 交换机透明传输 802.1x 认证报文

关于 802.1x 认证更详细的描述，可以参见 IEEE 802.1x 标准文档、RFC2869 和支持 802.1x 的华为网络设备的用户手册。

在经过了 802.1x 认证之后，用户就被允许访问网络资源，进行后续的上网过程，同时运营商也可以对该用户进行计费操作。

📖 **说明：**

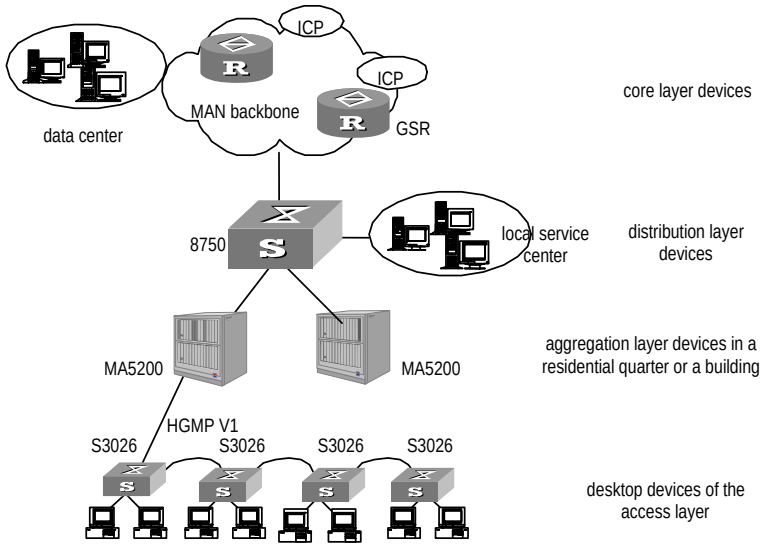
除了提供 802.1x 认证，华为公司还提供 portal 认证、Web 认证等方式对用户进行认证。对于这些认证的数据交换过程，可以参见相关的技术文档和支持这些功能的华为网络设备的用户手册。

下面引入一个问题：如果需要限制某些用户的上网时段；限制某些用户的带宽，例如某些用户虽然使用 10Mbit/s 的带宽和交换机相连，但是他只付了 2Kbit/s 带宽的费用。对于运营商来说，该怎样去控制网络设备适应不同的需求呢？可以通过人工关闭某个交换机的端口、到每个交换机上进行限制带宽的配置等满足这些需求，但是这样费时费力，不能满足可运营、可管理网络的需求。华为公司充分考虑了这种需求，为运营商提供了电信级的用户管理和运营能力。下面简单介绍在这种网络中的数据转发流程。

2. 在可运营、可管理网络中对用户进行集中管理

(1)　MA5200＋S3026 的组网方案

第一种方案：对前面小区的组网重新设计，利用“MA5200”加“S3026”进行组网。S3026 和 MA5200 之间的通信可通过 HGMP V1 来承载。通过 HGMP V1，MA5200 可以实现对 S3026 的集中管理；MA5200 可以通过上行高速口直接连接到 8750 或者直接连接到城域网或骨干网，多台 S3026 直接挂在 MA5200 的 100Mbit/s 以太网光接口上，然后 S3026 连接到小区用户桌面计算机上。



图A-10 通过 MA5200 实现电信级的用户管理和运营

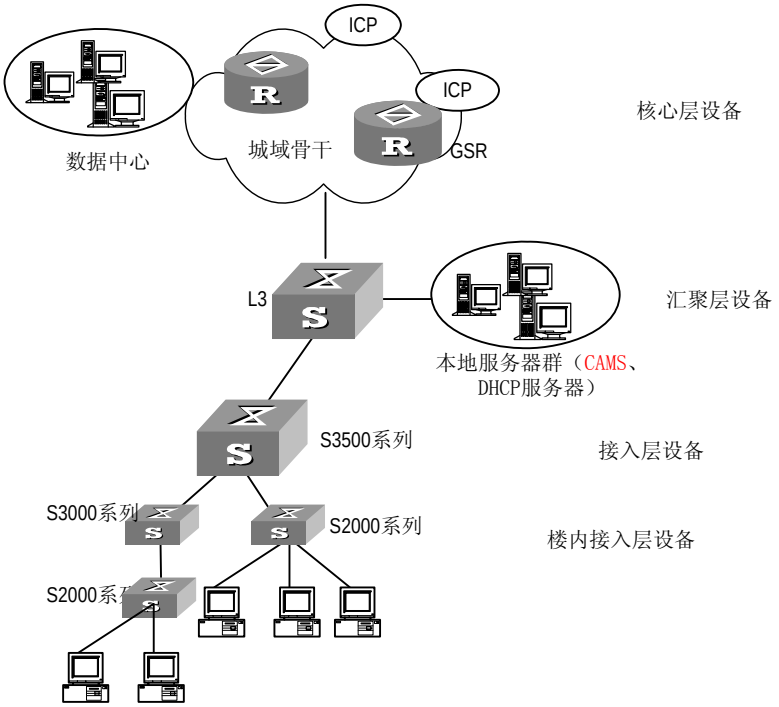
MA5200 可以对上网用户进行认证、授权、计费的功能，同时可以对用户使用的带宽、上网的时段进行控制，对用户进行按时按量计费，使之既有以太网接入经济、成熟的特色，又有电信级的用户管理和运营能力。

MA5200 可以在本地实现对上网用户进行认证、授权、计费，也可以把认证、授权、计费交给 RADIUS 服务器来做，这由 MA5200 上的配置所决定。

MA5200 将对用户的上网时段限制等配置信息通过 HGMP 报文直接下发到用户相连的 S3026 交换机上，并可以实现基于用户的带宽限制，从而实现对所有用户的集中管理。MA5200 的详细配置可以参见 MA5200 的用户手册。

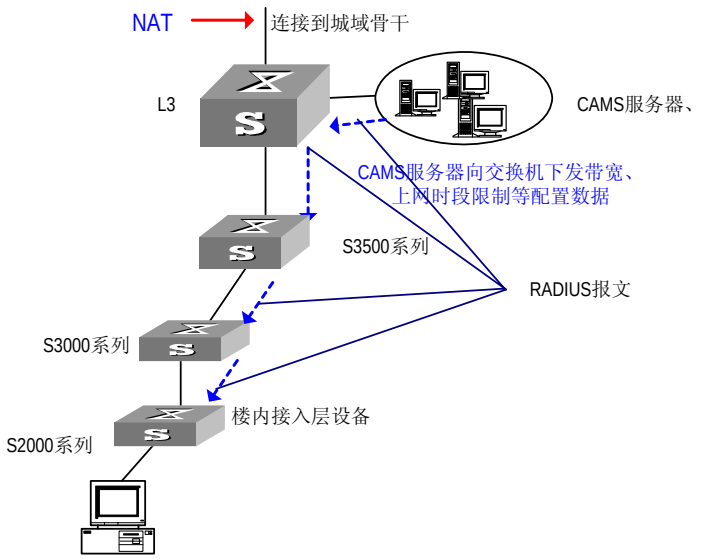
(2)　使用 CAMS 构造电信级交换网络

第二种方案，利用华为公司的 CAMS 服务器，实现电信级的可运营、可管理的交换网络。



图A-11 利用 CAMS 构造电信级交换网络

在小区的数据中心增加 CAMS 服务器。CAMS 服务器可以把对用户的上网时段限制等配置直接下发到各个交换机上，并且可以实现基于用户的带宽限制，从而实现对所有用户的集中管理。



图A-12 CAMS 下发配置数据的过程

📖 说明：

CAMS 下发的配置数据在缺省情况下封装在标准的 RADIUS 协议报文中。如果用户在交换机上作了如下配置之后：
Quidway(config-radius-huawei)#server-type huawei
CAMS 下发的配置数据将封装在华为扩展的 RADIUS 协议报文中。

同时 CAMS 服务器可以实现对用户的认证、授权、计费等功能，使网络具备电信级的可运营、可管理能力。对用户进行 802.1x 认证的过程和前面讲述的认证过程是一样的，只不过 RADIUS 服务器被 CAMS 服务器代替。

📖 说明：

CAMS 支持多设备，多业务，多协议，实现宽窄带的一体化的管理。它不会仅对一个小区网络提供服务，它在网络中的位置应该位于城域网的数据中心。此时它向交换机下发配置数据和 802.1x 认证的过程基本上没有改变，只是数据在小区和城域网之间需要进行一次 NAT 转换。

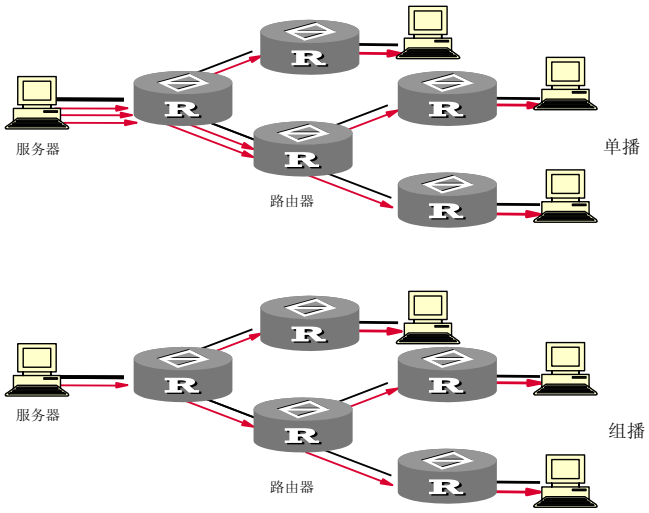
A.4 组播业务

宽带网络支持视频点播等业务。如果仅在网络层实现组播，则组播数据将在二层交换网络中进行广播，既浪费了大量的带宽，而且给网络设备带来巨大冲击，很可能会引起网络设备瘫痪。华为 Quidway 系列路由器和以太网交换机都支持组播特性，在网络层和数据链路层都实现了组播，解决了上述问题。

A.4.1 IP 组播

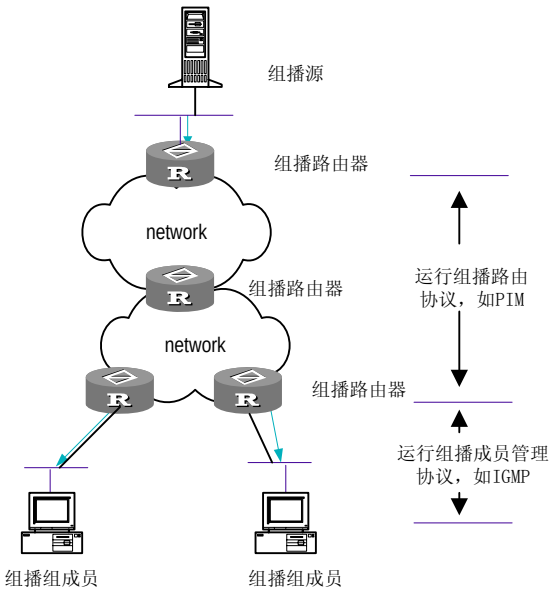
IP 组播是一种节省带宽的技术，它把一个数据流同时传送给许多接收者，组播源将需要传播的数据包发送一次，被传递的数据包在网络关键节点处不断地进行复制和分发。通过组播方式，数据包能被准确高效地传送到每个数据包接收者。IP 组播可以减少大量网络的流量。

IP 组播数据的转发和单播数据的转发如下图所示。



图A-13 单播与组播传送数据的对比

成功的进行组播需要组播路由协议和组播成员管理协议相互配合。组播路由协议负责维护组播路由信息，它跟踪、了解哪些组播报文需要在路由器之间转发，进而将组播报文发送到与组播路由器之间相连的局域网。组播成员管理协议是组播成员管理的协议，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。所有参与组播的主机必须实现组播成员管理协议，组播成员管理协议是 IP 组播路由协议的直接支持协议。



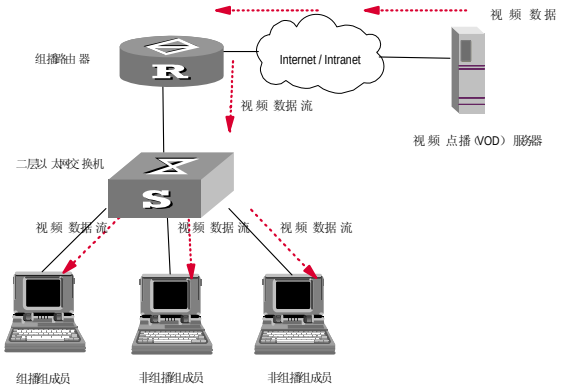
图A-14 IP 组播示意图

如上图所示，组播数据在组播路由器之间根据组播路由协议维护的路由表进行转发，在组播数据接收者和其相邻的组播路由器之间则根据组播成员管理协议维护的成员关系进行转发。

要了解组播协议更详细的描述，请参见 RFC 文档（如 RFC1112、RFC2236 等）和相关产品的用户手册。

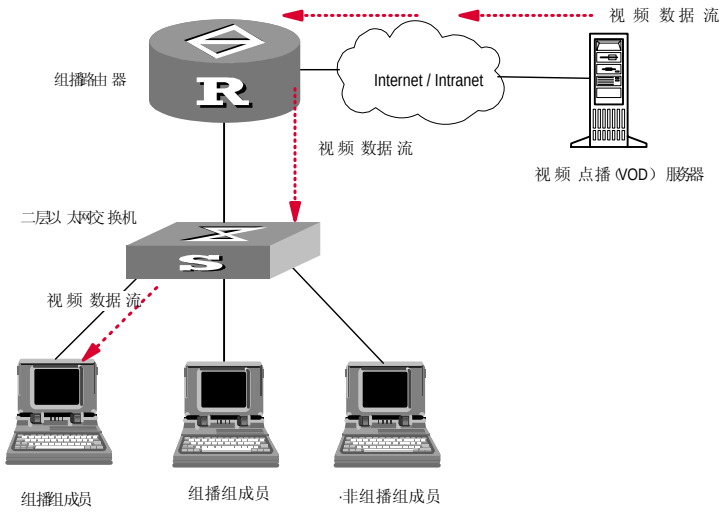
A.4.2 二层组播

在实现 IP 组播后，组播数据进入局域网后将在局域网内进行广播。这将造成网络带宽的极大浪费，同时也对网络设备带来很大冲击。华为 Quidway 系列以太网交换机实现了二层组播协议，使报文在二层也实现组播，从而解决了上述问题。



图A-15 没有实现二层组播时组播报文的传播过程

实现了二层组播以后，组播数据的转发流程如下图所示：



图A-16 实现二层组播后组播报文传播过程

二层组播协议是在交换机上维护二层组播转发表，表项由组播组、该组播组的转发端口列表等构成，这样，组播数据只会发送到连接有组播组成员的端口上。

关于二层组播的详细描述可以参见相应路由器和交换机的用户手册和相关技术文档。