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

文件系统实现的主要功能为管理存储设备。

文件系统为存储设备提供文件系统及文件、目录的管理，包括创建文件系统，创建、删除、修改、更名文件和目录，以及显示文件的内容。单级目录名或文件名最多支持 64 个字符。

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。

请在特权用户模式下进行下列配置。

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、彻底删除回收站中的文件、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。

请在特权用户模式下进行下列配置。

表1-2 文件操作

操作	命令
删除文件	**delete** *file-url*
恢复删除文件	**undelete** *file-url*
彻底删除回收站中的文件	**squeeze** *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。

请在特权用户模式下进行下列配置。

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 文件系统操作

用户通过命令可以修改当前文件系统的提示方式。

请在全局配置模式下进行下列配置。

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** }

1.1.6 文件系统使用举例

！**用户通过命令可以修改当前文件系统的提示方式。**

Quidway# format flash:

```
All sectors will be erased, proceed? [confirm]y
Format flash: completed
```

Quidway# cd flash:/

Quidway# pwd

```
flash:/
```

Quidway# mkdir test

Quidway# dir

```
Directory of *
0   drw-         0  Mar 09 2002 12:01:44   test
523776 bytes total (476160 bytes free)
```

1.2 配置文件管理

1.2.1 配置文件内容及格式

配置文件为一文本文件，其格式要求如下：

- **以命令格式保存。**
- **为了节省空间，只保存非缺省的常数（各配置参数的缺省值请详见以后各章节）。**
- **命令的组织以命令模式为基本框架，同一命令模式的命令组织在一起，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）。**
- **节的顺序安排通常为：全局配置、物理端口配置、逻辑接口配置、路由协议配置等。**
- **以 end 为结束。**

1.2.2 查看 S2000 系列以太网交换机的当前配置和起始配置

S2000 系列以太网交换机上电时，系统从 Flash 中读取配置文件，进行初始化工作，因此将 Flash Memory 中配置文件称为起始配置，如果 Flash Memory 中没有配置文件，则系统用缺省参数初始化。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。

请在除普通用户模式以外的所有其它配置模式下进行下列配置。

表1-5 查看 S2000 系列以太网交换机的配置

操作	命令
查看 S2000 系列以太网交换机的起始配置	**show startup-config**
查看 S2000 系列以太网交换机的当前配置	**show running-config**

📖 **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 S2000 系列以太网交换机的当前配置，为了使当前配置能够作为系统下次上电时的起始配置，需要用 write 命令保存当前配置到 Flash Memory 中。

请在特权用户模式下进行下列配置。

表1-6 保存当前配置

操作	命令
保存当前配置	**write**

1.2.4 擦除 Flash Memory 中配置文件

用 erase 命令可以擦除 S2000 系列以太网交换机 Flash Memory 中的配置文件，配置文件被擦除后，系统下次上电将采用缺省的配置参数进行初始化，在以下几种情况下，可以擦除 Flash Memory 中配置文件：

- 在 S2000 系列以太网交换机的软件升级之后，可能会引起系统软件和配置文件不匹配。
- 发现 Flash Memory 中的配置文件遭到破坏，如加载了错误的配置文件。

请在特权用户模式下进行下列配置。

表1-7 擦除 Flash 中 Memory 配置文件

操作	命令
擦除 Flash Memory 中配置文件	**erase**

1.3 FTP 配置

1.3.1 FTP 简介

FTP 协议在 TCP/IP 协议族中属于应用层协议，主要向用户提供远程主机之间的文件传输，FTP 协议基于相应的文件系统实现。

S2000 系列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，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 程序建立与服务器的连接后，可以输入 FTP 命令建立与远程 FTP Server 的连接并访问远程服务器上的文件。

1.3.2 FTP 服务器配置任务列表

- 启动 FTP 服务器
- 配置 FTP 服务器的验证和授权
- 配置 FTP 服务器的运行参数
- FTP 服务器的监控和维护

1.3.3 启动/关闭 FTP 服务器

请在全局配置模式下进行下列配置。

表1-8 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	**no 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。

1.3.4 配置 FTP 服务器的验证和授权

FTP 服务器的授权信息是提供给 FTP 用户的顶级工作目录。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。

FTP 服务器的验证和授权配置举例：

例：配置 FTP 用户名为 quidway，口令为 huawei（明文），授权工作目录为 c：/ftp/quidway（S2000 系列以太网交换机文件系统支持的路径名）。

！在全局配置模式下，配置 FTP 用户的验证信息。

Quidway(config)# user quidway password 0 huawei

！在全局配置模式下，配置 FTP 用户的授权信息。

Quidway(config)# user quidway ftp-directory c:/ftp/quidway

1.3.5 配置 FTP 服务器的运行参数

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 用户的服务请求，则断开与该 FTP 客户端的连接。

请在全局配置模式下进行下列配置。

表1-9 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	**no ftp timeout**

缺省情况下，超时断连时间为 30 分钟。

1.3.6 FTP 服务器的监控与维护

FTP 服务器提供以下命令，显示 FTP 服务器的运行状态和当前登录的 FTP 用户。

请在除普通用户模式以外的所有其它配置模式下进行下列操作。

表1-10 FTP 服务器的监控与维护

操作	命令
查看 FTP 服务器	**show ftp-server**
查看登录的 FTP 用户	**show ftp-user**

show 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。**show ftp-user** 显示登录的 FTP 用户的详细情况。

(1) 显示当前 FTP 服务器的配置情况。

Quidway# show ftp-server

```
Ftp server is running
Max user number       5
User count            0
Timeout(minute)       30
```

以上显示信息表示：FTP 服务器已经启动，支持同时登录的最大用户数为 5 个，现在登录的用户数为 0 个，FTP 用户的超时时间为 30 分钟。

(2) 显示当前 FTP 用户的配置情况。

Quidway# show ftp-user

```
username      host            port     topdir          idle
quidway       10.110.3.5      1074     c:/quidway      2
```

以上显示信息表示：有一个 FTP 用户和 FTP 服务器建立了连接，该用户的用户名为 quidway，远地主机 IP 地址为 10.110.3.5，远地端口号为 1074，授权目录为 c:/quidway，现在已经有 2 分钟没有向 FTP 服务器发送服务请求。

1.3.7 FTP 客户端介绍

FTP 客户端，作为 S2000 系列以太网交换机提供给用户的一个附加功能，它没有任何配置功能，是一个应用模块。用户作为 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，例如：建立、删除目录等。

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，适用于客户机和服务器之间不需要复杂交互的环境，例如在系统启动时使用 TFTP 协议来获取系统的内存映像。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包，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包，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。S2000 系列以太网交换机提供了 TFTP 客户端的功能。

1.4.2 TFTP 配置任务列表

TFTP 主要配置任务列表如下：

- 配置文件传输模式
- 用 TFTP 下载文件
- 用 TFTP 上传文件

1.4.3 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。

请在全局配置模式下进行下列配置。

表1-11 配置文件传输模式

操作	命令
设置 TFTP 为 ASCII 码传输模式或二进制传输模式	**tftp** { **ascii** | **binary** }

缺省情况下，TFTP 传输文件为二进制模式。

1.4.4 用 TFTP 下载文件

请在全局配置模式下进行下列配置。

表1-12 用 TFTP 下载文件

操作	命令
用 TFTP 获取文件	**tftp get** *//A.A.A.A/xxx.yyy mmm.nnn*

1.4.5 用 TFTP 上传文件

请在全局配置模式下进行下列配置。

表1-13 用 TFTP 上传文件

操作	命令
用 TFTP 保存文件	**tftp put** *mmm.nnn //A.A.A.A/xxx.yyy*

1.5 系统 IP 配置

1.5.1 系统 IP 简介

1. 管理 VLAN

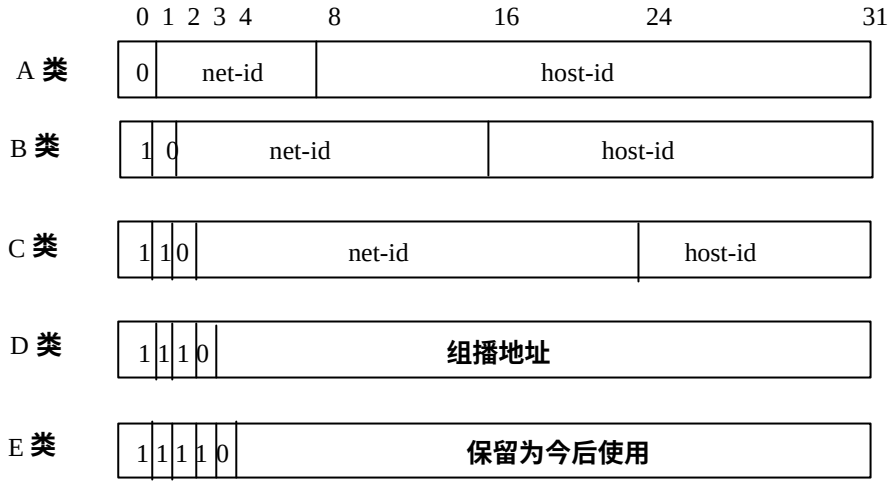
在 S2000 系列以太网交换机中，只有管理 VLAN 才需要配置 IP 地址。管理 VLAN 就是对访问交换机网管的端口增加了 VLAN 设置功能。没有管理 VLAN 和不设置管理 VLAN 时，通过交换机的任意端口都可以访问交换机的网管，这时网络中存在的大量广播报文也同时被送到网管，由交换机的 CPU 进行相关处理。由于交换机的 CPU 处理能力有限，可能无法处理所有的报文，未经处理的报文就会堆积在交换芯片中，从而引发网管端口的堵塞。如果端口没有输出队列的限制功能还可能引起整个芯片的交换阻塞问题。有了管理 VLAN 之后可以通过管理 VLAN 的设置来限制端口对网管的访问，只有包含在管理 VLAN 内的端口才可以访问网管，其余端口的任何报文都不会被送到网管，这样就避免了网管堵塞而可能引起的交换阻塞的问题，同时也极大地降低了 CPU 的负荷。

2. IP 地址

所谓 IP 地址，是指分配给连接在 Internet 上的主机的一个唯一的 32 比特地址。IP 地址一般由两部分组成：第一部分为网络号码，第二部分为主机号码。IP 地址的结构使我们可以在 Internet 上方便地进行寻址。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 地址的管理以及组网，Internet 的 IP 地址分成五类。如图 1-1 所示，IP 地址由下列两个字段组成：

- 网络号码字段（net-id）；网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。
- 主机号码字段（host-id）。



net-id—网络号码，host-id—主机号码

图1-1 五类 IP 地址

D 类地址是一种组播地址，主要是留给 Internet 体系结构委员会 IAB（Internet Architecture Board）使用。E 类地址保留在今后使用。目前大量使用中的 IP 地址属于 A、B、C 三种中的一种。

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1-14 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	主机号码全为 0 的 IP 地址表示该网络的地址，用于网络路由； 主机号码全为 1 的 IP 地址表示广播地址，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

网络类型	地址范围	用户可用的 IP 网络范围	说明
			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	主机号码全为 0 的 IP 地址表示该网络的地址，用于网络路由； 主机号码全为 1 的 IP 地址表示广播地址，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	主机号码全为 0 的 IP 地址表示该网络的地址，用于网络路由； 主机号码全为 1 的 IP 地址表示广播地址，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 ～ 247.255.255.255	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。

IP 地址有一些重要的特点：

(1) IP 地址是一种非等级的地址结构，和电话号码的结构不一样，也就是说，IP 地址不能反映任何有关主机位置的地理信息。

(2) 当一个主机同时连接到两个网络上时（作 S2000 系列交换机用的主机即为这种情况），该主机就必须同时具有两个不同的 IP 地址，其网络号码 net-id 是不同的，这种主机成为多地址主机（multihomed host）。

(3) 按照 Internet 的观点，用转发器或网桥连接起来的若干个局域网仍为一个网络，因此这些局域网都具有同样的网络号码 net-id。

在 IP 地址中，所有分配到网络号码 net-id 的网络（不管是小的局域网还是很大的广域网）都是平等的。

从 1985 年起，为了使 IP 地址的使用更加灵活，只分配 IP 地址的网络号码 net-id，而后面的主机号码 host-id 则是受本单位控制。即某个单位申请到 IP 地址时，实际上只是拿到了一个网络号码 net-id，具体的各个主机号码 host-id 则由该单位自行分配，只要做到在该单位管辖的范围内无重复的主机号码即可。当一个单位的主机很多而且分布在很大的地理范围时，为了便于管理，可将单位内部的主机号码再进一步划分为多个子网。需要注意的是，子网的

划分纯属本单位内部的事，在本单位以外是看不见划分的操作。从外部看，这个单位只有一个网络号码。只有当外面的报文进入到本单位范围后，本单位的路由器才根据子网络号码再进行选路，找到目的主机。

如图 1-2 所示，为一个 B 类 IP 地址划分子网情况，其中子网掩码由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码和子网络号码字段，而“0”对应于主机号码字段。

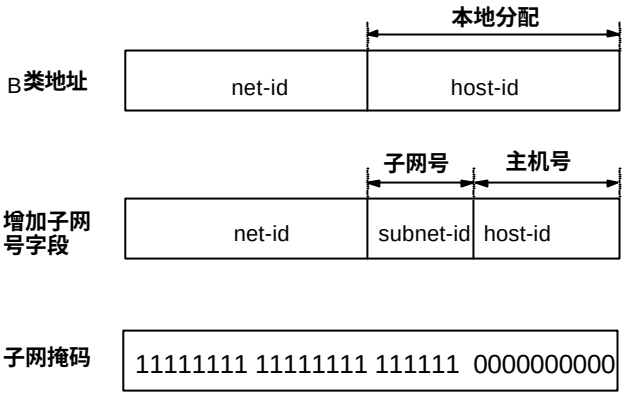


图1-2 IP 地址子网划分

多划分出一个子网络号码字段是要付出代价的。举例来说，本来一个 B 类 IP 地址可以容纳 65534 个主机号码。但划分出 6bit 长的子网字段后，最多可有 62 个子网（去掉全 1 和全 0 的子网络号码）。每个子网有 10bit 的主机号码，即每个子网最多可有 1022 个主机号码。因此主机号码的总数是 62×1022=63364 个。比不划分子网时要少了一些。

若一个单位不进行子网的划分，则其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。因此，对于 A，B 和 C 类的 IP 地址，其对应子网掩码的默认值分别为 255.0.0.0；255.255.0.0.和 255.255.255.0。

一台路由器用来连接多个子网，具有多个子网的 IP 地址。上面讲的 IP 地址还不能直接用来进行通信。这是因为：

- IP 地址只是主机在网络层中的地址，若要将网络层中传送的数据报交给目的主机，必须知道该主机的物理地址。因此必须将 IP 地址解析为物理地址。
- 用户平时不愿意使用难于记忆的 IP 地址，而是愿意使用易于记忆的主机名，因此也需要将主机名解析为 IP 地址。

图 1-3 表示了主机名、IP 地址和物理地址之间的关系。

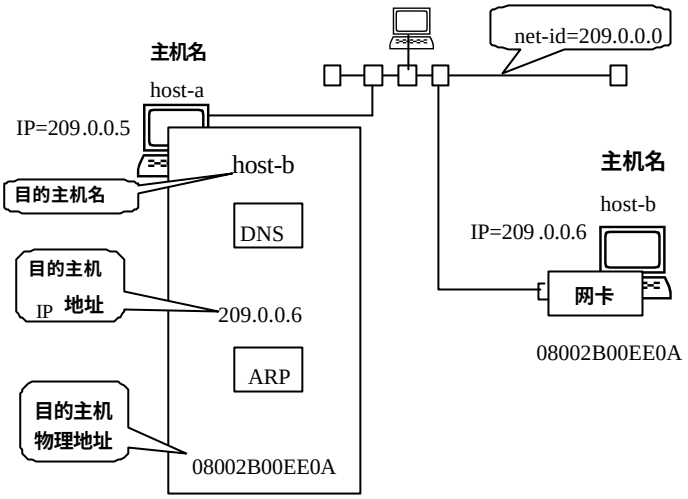


图1-3 主机名、IP 地址和物理地址之间的关系

3. ARP

ARP **即地址解析协议，主要用于将** IP **地址解析为以太网** MAC **地址。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。**

1.5.2 系统 IP 配置任务列表

- **创建/删除管理** VLAN **接口**
- **给管理** VLAN **接口指定/删除** IP **地址和掩码**
- **配置缺省网关**

1.5.3 进入/删除管理 VLAN 接口

此任务使用命令 interface { *interface_type interface_num* | *interface_name* } **实现，此时参数** *interface_type* **取 vlan-interface，***interface_num* **为** *vlan_id***。**

请在全局配置模式下，进行下列配置。

表1-15 **创建/删除** VLAN **接口**

操作	命令
进入 VLAN **接口配置模式**	**interface vlan-interface** *vlan_id*
删除 VLAN **接口**	**no interface vlan-interface** *vlan_id*

需要注意的是：只有在 VLAN **已经建立后，才能创建** VLAN **的路由接口。**

参数 *vlan_id* 的取值范围为 1～4000。

1.5.4 给管理 VLAN 接口指定/删除 IP 地址和掩码

通过给管理 VLAN 接口指定 IP 地址，使 S2000 系列以太网交换机可以通过 IP 协议被访问。

请在全局配置模式下，进行下列配置。

表1-16 给管理 VLAN 接口指定/删除 IP 地址和掩码

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	**no ip address** [*ip-address net-mask*]

通过掩码来标识 IP 地址包含的网络号，例如：S2000 系列交换机管理 VLAN 接口的 IP 地址是 129.9.30.42，掩码是 255.255.0.0，将 IP 地址与掩码相“与”后，可知 S2000 系列交换机管理 VLAN 接口所在网段的地址为 129.9.0.0。

缺省情况下，管理 VLAN 接口无 IP 地址。

1.5.5 配置缺省网关

请在全局配置模式下，进行下列配置。

表1-17 配置静态路由

操作	命令
增加一条静态路由	**ip route** *ip-address* { *mask* | *mask-length* } { *interface_name* | *gateway-address* } [**preference** *preference-value*] [**reject** | **blackhole**]
删除一条静态路由	**no ip route** *ip-address* { *mask* | *mask-length* } [*interfacce-name* | *gateway-address*] [**preference** *value*]

需要注意的是，S2000 系列以太网交换机不支持属性 reject 和 blackhole 选项。

(1) 路由配置

S2000 系列以太网交换机可以且只可以配置一条路由用于通过网络对交换机进行访问。配置路由时使用 reject 和 blackhole 参数都是没有意义的。

1.5.6 系统 IP 的监控和维护

请在除普通用户模式外的所有配置模式下，进行下列操作。

表1-18 系统 IP 地址的监控与维护

操作	命令
显示路由表信息	show ip route

第2章 设备管理

2.1 MAC 地址表管理

2.1.1 MAC 地址表管理简介

S2000 系列以太网交换机维护着一张用于转发报文的 MAC 地址表。这张表的表项包含了设备的 MAC 地址及与此设备相连的交换机端口号。对于目的 MAC 地址能够在地址表中查到的报文，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处理。

S2000 系列以太网交换机具有 MAC 地址学习的功能。如果接收到的报文的源 MAC 地址在地址表中不存在，系统就会将此报文的源 MAC 地址及接收此报文的端口号作为一个新的表项添加到 MAC 地址表中。

可以人工配置 MAC 地址表项。管理员可以根据实际网络情况配置 MAC 地址表，添加或修改的表项可以是静态表项或者动态表项。

S2000 系列以太网交换机提供 MAC 地址老化的功能。一个设备在一定时间内没有发送任何报文，系统就会把与此设备相关的 MAC 地址表项删除。MAC 地址老化只对学习到的或者用户配置的可老化（动态）MAC 地址表项起作用。

2.1.2 MAC 地址表管理配置任务列表

MAC 地址表管理配置任务列表如下：

- 设置 MAC 地址表项
- 设置系统 MAC 地址老化设置
- 关闭/开启 MAC 地址学习功能

2.1.3 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。

请在全局配置模式下进行下列配置。

表2-1 设置 MAC 地址表项

操作	命令
添加/修改地址表项	**mac-address-table** { **static** | **permanent** | **blackhole** | **dynamic** } *hw-addr* **interface** { *interface_name* | *interface_type interface_num* }
删除地址表项	**no mac-address-table** [**static** | **permanent** | **blackhole** | **dynamic**] [[*hw-addr*] **interface** [*interface_name* | *interface_type interface_num*]]

在删除动态表项时会同时把学习到的地址表项删除。

2.1.4 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。一个设备在老化时间的时长范围内没有发送任何报文，其对应的 MAC 地址表项就会被删除。设置过短的老化时间会造成 MAC 地址表项很快就被删除，这样与相应地址表项匹配的数据报文会因为找不到目的 MAC 地址而被广播，从而影响交换机的运行性能；设置过长的老化时间会导致不再使用的 MAC 地址表项在地址表中长期存在，容易导致交换机的 MAC 地址表资源耗尽，交换机无法根据网络的变化更新 MAC 地址表，造成大量报文找不到目的 MAC 地址而被广播。因此设置合适的老化时间是有效实现 MAC 地址老化功能的充要条件。一般情况下，推荐使用老化时间的缺省值 300 秒。

请在全局配置模式下进行下列配置。

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-table** { **aging-time** *aging_time* | **table-full** }
恢复 MAC 地址老化时间的缺省值	**no mac-address-table aging-time**

地址老化只对学习到的或者用户配置可老化（动态）的 MAC 地址表项起作用。参数 *aging_time* 的缺省值为 300 秒。使用参数 **table-full** 时表示不对 MAC 地址表项进行老化。

另外，此命令为全局命令，作用于全部端口上。在千兆以太网端口配置模式下也有作用于单个端口的、起到同样效果的命令，具体细节请参考端口配置部分章节。

2.1.5 关闭全局 MAC 地址学习功能

S2000 系列以太网交换机的地址学习功能使得交换机在学习到 MAC 地址后，再收到以此 MAC 地址为目的 MAC 地址的数据报文时将不再对其广播转发。关闭地址学习功能是为了保证交换机的安全。例如有人使用不同源 MAC 地址的帧攻击交换机会导致交换机 MAC 地址表资源耗尽，关闭 MAC 地址学习功能可以有效防止这种情况。

请在全局配置模式下进行下列配置。

表2-3 关闭/开启 MAC 地址学习功能

操作	命令
关闭 MAC 地址的学习功能	mac-address-table mac-learning disable
恢复学习 MAC 地址	no mac-address-table mac-learning disable

缺省情况下，开启 MAC 地址学习功能。

2.1.6 关闭端口 MAC 地址学习功能

以太网交换机可以关闭单个端口的 MAC 地址学习功能

请在端口配置模式下进行下列配置。

表2-4 关闭/开启 MAC 地址学习功能

操作	命令
关闭 MAC 地址的学习功能	mac-address-table mac-learning disable
恢复学习 MAC 地址	no mac-address-table mac-learning disable

缺省情况下，开启 MAC 地址学习功能。

2.1.7 MAC 地址表管理的监控与维护

请在特权用户模式下进行下列操作。show mac-address-table 命令还可以在除了普通用户模式以外的所有其它配置模式下使用。

表2-5 MAC 地址表管理的监控与维护

操作	命令
显示地址表信息	**show mac-address-table** [**static** | **permanent** | **blackhole | dynamic**] [[**interface** { *interface_name* | *interface_type interface_num* }] [**vlan** *vlan-id*] | **all**]
显示地址表动态表项的老化时间	**show mac-address-table aging-time**
显示系统和端口动态学习 MAC 地址的能力	**show mac-address-table mac-learning** [*interface_type interface_num* | *interface_name*]
打开地址表管理的调试信息开关	**debug mac-address-table**
关闭地址表管理的调试信息开关	**no debug mac-address-table**

(1) 显示地址表信息

！显示地址表中 MAC 地址为 00e0.fc01.0101 的地址表项的信息。

Quidway(config)# show mac-address-table 00e0.fc01.0101

```
MAC ADDR       VLAN ID   STATE          PORT INDEX       AGING TIME(s)
00e0.fc01.0101    1      Config static  Ethernet0/1          NOAGED
```

以上显示信息表示：MAC 地址为 00e0.fc01.0101 的数据包将从 VLAN1 的 Ethernet 0/1 端口转发，这个表项被配置为静态表项，没有老化时间。

(2) 显示地址表动态表项的老化时间

！显示地址表中动态表项的老化时间。

Quidway(config)# show mac-address-table aging-time

```
mac-address-table aging-time: 300s
```

以上显示信息表示：MAC 地址表中动态表项的老化时间为 300 秒。

(3) 显示端口动态学习 MAC 地址的能力

！显示千兆以太网端口 Ethernet 0/1 动态学习 MAC 地址表项的能力。

Quidway(config)# show mac-address-table mac-learning ethernet 0/1

```
mac-address learning status of the switch: enable

PortName              Learning Status
Ethernet0/1           enable
```

以上显示信息表示：本机的动态学习 MAC 地址能力为启动状态，端口 Ethernet 0/1 能够动态学习 MAC 地址。

2.1.8 地址表管理典型配置举例

1. 组网需求

能够通过 Console 口或 Telnet 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

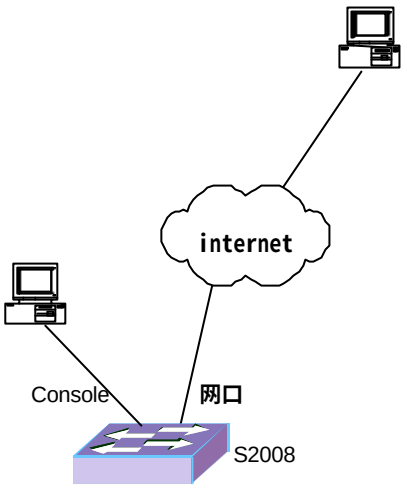


图2-1 地址表管理典型配置组网图

3. 配置步骤

！通过 Console 口启动超级终端或 Telnet 到交换机，并进入交换机全局配置模式。

！增加一个 MAC 地址（指出所属 VLAN、端口、状态）。

Quidway(config)# mac-address-table static 00e0.fc35.dc71 interface ethernet 0/2 vlan 1

！地址老化时间设置为 500 秒。

Quidway(config)# mac-address-table aging-time 500

！在所有配置模式下察看 MAC 地址配置。

Quidway(config)# show mac-address-table interface ethernet 0/2

```
MAC ADDR           VLAN ID STATE      PORT INDEX         AGING TIME(s)
00-e0-fc-35-dc-71  1       Static     Ethernet0/2           NOAGED
00-e0-fc-17-a7-d6  1       Learned    Ethernet0/2           300
00-e0-fc-5e-b1-fb  1       Learned    Ethernet0/2           300
```

```
00-e0-fc-55-f1-16  1       Learned    Ethernet0/2          300
```

2.2 设备管理

2.2.1 设备管理简介

S2000 系列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。

2.2.2 设备管理配置任务列表

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监控和维护。

设备管理的配置任务包括：

- 复位单板
- 指定交换机下次启动采用的 APP
- 升级 bootrom

2.2.3 复位单板

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单板。

请在特权用户模式下进行下列配置：

表2-6 复位单板

操作	命令
复位单板	**reboot**

2.2.4 指定交换机下次启动采用的 APP

当 Flash 中有多个 app 时，可以指定交换机下次启动所采用的 app。

请在特权用户模式下进行下列配置：

表2-7 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 bootldr file-url**

2.2.5 升级 bootrom

使用本命令在系统运行过程中使用 Flash 中的 bootrom 程序升级 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。

请在特权用户模式下进行下列配置：

表2-8 升级 bootrom

操作	命令
升级 bootrom	**boot bootrom file-url**

2.2.6 设备管理的监控与维护

请在特权用户模式或全局配置模式下进行下列操作。其中，show 系列命令还可以在除普通用户模式以外的所有其它配置模式下使用。

表2-9 设备管理的监控与维护

操作	命令
清除流经各子板的以太网帧的统计信息（全局配置模式）	**clear slot statistics**
显示各单板的模块类型及工作状态	**show device**
显示内置风扇的工作状态	**show fans state**
显示流经各子板的以太网帧的统计信息	**show slot statistics**
显示下次启动采用的 APP	**show bootvar**
打开设备管理调试开关	**debug device event**
关闭设备管理调试开关	**no debug device event**

以上各命令的具体使用方法及显示信息的细节描述请参见命令参考分册的相关章节。

(1) 显示各单板的模块类型及工作状态

！显示各单板的信息。

Quidway# show device

```
SlotNo SubSNo PortNum HdVer  FPGAVer BtSftVer AppSftVer AddrLM Type
Describ
   0      0       8   REV.A    NULL    1.1       001     SVL    1   MAIN
   0      1       1   NULL     NULL    NULL      NULL    SVL    10  STKD
```

以上信息表示（以第一行为例，其他行类似）：物理板号 SlotNo 为 0 的单板，子板号 SubSNo 为 0 的单板，子板号 SubSNo 为 0 表示主板（1 表示扩展的 FE 口子板号），端口个数为 8 个，硬件版本为 A 版本，FPGA 版本号为 NULL，BOOTROM 软件版本号为 1.1，应用软件版本号为 001，地址学习模式 SVL，接口板类型为 1 号类型，接口板类型描述为 MAIN。

第3章 系统维护

3.1 维护调试工具

3.1.1 show 命令查看系统状态和系统信息

show 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 show 命令请参见相关章节。下面只介绍一些有关系统的 show 命令。

请在除普通用户模式以外的所有其它配置模式下进行下列操作，其中 show version 还可在普通用户模式下进行。

表3-1 系统 show 命令

操作	命令
显示系统时钟	show clock
显示系统版本	show version
显示终端用户	show users
显示起始配置	show startup-config
显示当前配置	show running-config
显示调试开关状态	show debugging

(1) 显示系统版本。

Quidway# show version

```
Huawei Versatile Routing Platform Software
VRP (tm) Lanswitch Platform Software Version V100R002B09D001
Quidway S2403F Software Version V200R003B02D001, RELEASE SOFTWARE
Copyright (c) 2000-2002 By HUAWEI TECH CO., LTD.
Compiled Jun 18 2002 14:17:30

QuidwayS2403F with 62.5M Arm7 Processor
 24M    bytes SDRAM
8192K   bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.A
Bootrom Version is 1.1
```

```
[Subslot 0] 8 100BASET  Hardware Version is REV.A
[Subslot 1] 1  FTIU      Hardware Version is NULL
```

以上显示为 S2000 **系列以太网交换机软硬件版本信息。**

(2) **显示系统时钟。**

Quidway# show clock

```
16:47:17 UTC Fri 2002/3/15
```

其它 show **命令参见相关章节。**

3.1.2 系统基本配置及管理

系统基本配置和管理任务包括:

- **设置交换机主机名**
- **设置系统时钟**

请在全局配置模式下进行 hostname 命令的操作。请在特权用户模式下进行 clock set 命令的操作。

表3-2 **系统基本配置及管理**

操作	命令
设置交换机主机名	**hostname** *hostname*
设置系统时钟	**clock set** *HH:MM:SS YYYY/MM/DD*

！**设置某台** S2000 **系列以太网交换机的主机名为** Quidway2008A（**缺省为** Quidway，**最大长度为** 30 **个字符**）。

Quidway(config)# hostname Quidway2008A

！**设置系统时钟** 2003 **年** 1 **月** 1 **日** 0 **点** 0 **分** 0 **秒。**

Quidway# clock set 0:0:0 2003/01/01

3.1.3 网络连接的测试命令

1. ping

ping **主要用于检查网络连接及主机是否可达。**

请在特权用户模式或普通用户模式下进行下列操作。

表3-3 ping 命令

操作	命令
支持 IP 协议 ping	**ping** [-**a** *ip-address*] [**-c** *count*] [**-d**] [-**i** {*interface_type interface_num* | *interface_name* }][**ip**] [**-n**] [**-p** *pattern*] [**-q**] [**-r**][**-s** *packetsize*] [**-t** *timeout*] [**-v**] *host*

各选项及参数意义详见命令参考手册 ping **命令章节。**

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。**

Quidway# ping 202.38.160.244

```
ping 202.38.160.244 : 56 data bytes press CTRL-C to break
Reply from 202.38.160.244 : bytes=56 sequence=1 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=2 ttl=255 time = 2ms
Reply from 202.38.160.244 : bytes=56 sequence=3 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=4 ttl=255 time = 3ms
Reply from 202.38.160.244 : bytes=56 sequence=5 ttl=255 time = 2ms
--202.38.160.244 ping statistics--
5 packets transmitted
5 packets received
0% packet loss
round-trip min/avg/max = 1/2/3 ms
```

2. tracert

tracert **用于测试数据包从发送主机到目的地所经过的网关，它主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。**

tracert **的执行过程是：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。**

表3-4 tracert 命令

操作	命令
Trace Route	**tracert** [**-f** *first-TTL*] [**-m** *max-TTL*] [**-p** *port*] [**-q** *nqueries*] [**-w** *timeout*] *host*

该命令各选项及参数意义详见命令手册 tracert **命令章节。**

下面是应用 tracert **分析网络情况的例子。**

Quidway# tracert 35.1.1.48

```
traceroute to nis.nsf.net (35.1.1.48), 30 hops max, 56 byte packet
1  helios.ee.lbl.gov (128.3.112.1)  19 ms  19 ms  0 ms
2  lilac-dmc.Berkeley.EDU (128.32.216.1)  39 ms  39 ms  19 ms
3  ccngw-ner-cc.Berkeley.EDU (128.32.136.23)  39 ms  40 ms  39 ms
4  ccn-nerif22.Berkeley.EDU (128.32.168.22)  39 ms  39 ms  39 ms
5  128.32.197.4 (128.32.197.4)  40 ms  59 ms  59 ms
6  131.119.2.5 (131.119.2.5)  59 ms  59 ms  59 ms
7  129.140.70.13 (129.140.70.13)  99 ms  99 ms  80 ms
8  129.140.71.6 (129.140.71.6)  139 ms  239 ms  319 ms
9  129.140.81.7 (129.140.81.7)  220 ms  199 ms  199 ms
10  nic.merit.edu (35.1.1.48)  239 ms  239 ms  239 ms
```

从上面结果可以看出从源主机到目的地都经过了哪些网关，这对于网络分析是非常有用的。

Quidway# tracert 18.26.0.115

```
traceroute to allspice.lcs.mit.edu (18.26.0.115), 30 hops max
1  helios.ee.lbl.gov (128.3.112.1)  0 ms  0 ms  0 ms
2  lilac-dmc.Berkeley.EDU (128.32.216.1)  19 ms  19 ms  19 ms
3  lilac-dmc.Berkeley.EDU (128.32.216.1)  39 ms  19 ms  19 ms
4  ccngw-ner-cc.Berkeley.EDU (128.32.136.23)  19 ms  39 ms  39 ms
5  ccn-nerif22.Berkeley.EDU (128.32.168.22)  20 ms  39 ms  39 ms
6  128.32.197.4 (128.32.197.4)  59 ms  119 ms  39 ms
7  131.119.2.5 (131.119.2.5)  59 ms  59 ms  39 ms
8  129.140.70.13 (129.140.70.13)  80 ms  79 ms  99 ms
9  129.140.71.6 (129.140.71.6)  139 ms  139 ms  159 ms
10  129.140.81.7 (129.140.81.7)  199 ms  180 ms  300 ms
11  129.140.72.17 (129.140.72.17)  300 ms  239 ms  239 ms
12  * * *
13  128.121.54.72 (128.121.54.72)  259 ms  499 ms  279 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  ALLSPICE.LCS.MIT.EDU (18.26.0.115)  339 ms  279 ms  279 ms
```

对以上显示内容的相应说明如下：

表3-5 tracert 命令说明表

显示内容	内容说明
tracertroute to allspice.lcs.mit.edu (18.26.0.115)	表示将要到达的目的主机名及 IP 地址。
30 hops max	表示最大 TTL 字段为 30。
40 bytes packet	表示数据报 40 字节。
1	表示到达主机所经由的网关的序列号。
helios.ee.lbl.gov	表示经由网关名。
128.3.112.1	表示经由网关 IP 地址。
0 ms 0 ms 0 ms	表示三份数据报的 ICMP 报文分别在 0 ms、0 ms、0 ms 收到。

从上述结果中可以看出从源主机到目的主机经过了哪些网关，以及哪些网关出现了故障。

3.1.4 日志功能

1. SYSLOG 介绍

日志系统是 S2000 系列以太网交换机中不可或缺的一部分，它作为系统软件模块的信息枢纽而存在。日志系统接管大多数的信息输出，并且能够进行细致的分类，从而能够有效地进行信息筛选，它通过与 Debug 程序的结合，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。

S2000 系列以太网交换机的日志系统具有以下一些特性：

- 支持控制台（ Console ）、Telnet 终端和哑终端（ monitor ）、日志缓冲区（ logbuf ）、日志主机（ loghost ）、告警缓冲区（trapbuf）、SNMP 六个方向的日志输出。
- 日志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。

2. SYSLOG 配置

(1) 开启或关闭日志功能

请在全局配置模式下进行下列操作。

表3-6 开启或关闭日志功能

操作	命令
开启日志系统	logging on
关闭日志系统	no logging on

📖 **说明**:

syslog 缺省情况下处于开启状态．在 syslog 开启时，由于信息分类、输出的原因，特别是在处理信息较多时，对系统性能有一定的影响．

(2) 输出日志信息

目前，S2000 系列以太网交换机的日志系统，可以在六个方向输出各种日志信息：

- 通过 Console 口向本地控制台输出日志信息。
- 向远程 Telnet 终端或哑终端输出日志信息，此功能有助于远程维护。
- 在交换机系统内部分配适当大小的缓冲区，用于记录日志信息。
- 配置日志主机，日志系统直接将日志信息发往日志主机，并在其上以文件的形式保存起来，供随时查看。
- 在交换机内部分配适当大小的告警缓冲区，用于记录信息。
- 向 SNMP Agent 输出信息。

每个输出方向通过配置命令指定所需要的通道，所有信息经过指定通道的过滤，发送到相应的输出方向；可根据需要配置输出方向所使用的通道，以及配置通道的过滤信息，完成各类信息的过滤以及重定向。

请在全局配置模式下进行下列配置。

表3-7 输出日志信息

操作	命令
向 Console 方向输出信息	**set console channel** { *channel-number* | *channel-name* }
向 Telnet 终端或哑终端输出信息	**set monitor channel** { *channel-number* | *channel-name* }
向日志缓冲区输出信息	**set logging buffered** [**size** *buffersize*] [**channel** { *channel-number* | *channel-name* }]
取消向日志缓冲区输出信息	**no logging buffered**
向日志主机输出信息	**set logging host** *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	**no logging host** *host-ip-addr*
向告警缓冲区输出信息	**set logging buffered** [**size** *buffersize*] [**channel** { *channel-number* | *channel-name* }]
取消向告警缓冲区输出信息	**no trappings buffered**
向 SNMP 输出信息	**set snmp channel** { *channel-number* | *channel-name* }

目前，系统对每个输出方向缺省分配一个信息通道，它们是

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
日志缓冲区	4	logbuf
告警缓冲区	3	trapbuf
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，设置才会生效.

(3) SYSLOG 定义的优先级（severity）

SYSLOG 按信息的严重等级或紧急程度划分为八个等级，在按等级来进行日志信息过滤时，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。

表3-8 syslog 定义的优先级（severity）

严重等级	描述
emergencies	极其紧急的错误
alerts	需立即纠正的错误
critical	关键错误
errors	需关注但不关键的错误
warnings	警告，可能存在某种差错
notifications	需注意的信息
informational	一般提示信息
debugging	调试信息

！设置允许 PPP 协议日志信息等级为 debugging 及以上的信息从控制台输出。

Quidway(config)# enable source ppp type log level debugging channel console

(4) 定义信息通道的内容

请在全局配置模式下进行下列操作。

表3-9 定义信息通道的内容

操作	命令
向信息通道中添加对于某模块某类信息的过滤记录	**set source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log level** *severity* **state** *state*] [**trap level** *severity* **state** *state*] [**debug level** *severity* **state** *state*]
删除信息通道中关于某模块或全部模块的内容	**no set 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。

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，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.

(5) **日志主机的配置**

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/config

#touch /var/log/Quidway/security

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.crit /var/log/Quidway/config

#Quidway security messages

local5.notice /var/log/Quidway/security

📖 **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.

第三步：当日志文件 config **和** security **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.

(6) **日志配置综合示例**

- **配置控制台日志输出**

！**开启日志系统。**

Quidway(config)# logging on

！**配置控制台日志输出，允许** RSTP **模块的日志输出，严重等级限制为** emergencies~debugging**。**

Quidway(config)# set console channel console

Quidway(config)# set source rstp channel 6 log level debugging

！**打开** rstp **模块的调试开关。**

Quidway# debug rstp all

- **配置日志主机**

交换机侧配置如下：

！**开启日志系统。**

Quidway(config)# logging on

！**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** RSTP **和** IP**。**

Quidway(config)# set logging host 202.38.1.10 language english

Quidway(config)# set source rstp channel 5 log level informational

Quidway(config)# set source ip channel 4 log level informational

主机侧配置请参见“日志主机配置”章节。

3.1.5 调试功能

S2000 **系列以太网交换机的命令行接口提供了种类丰富的调试功能，对于所支持的各种协议和功能，基本上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。

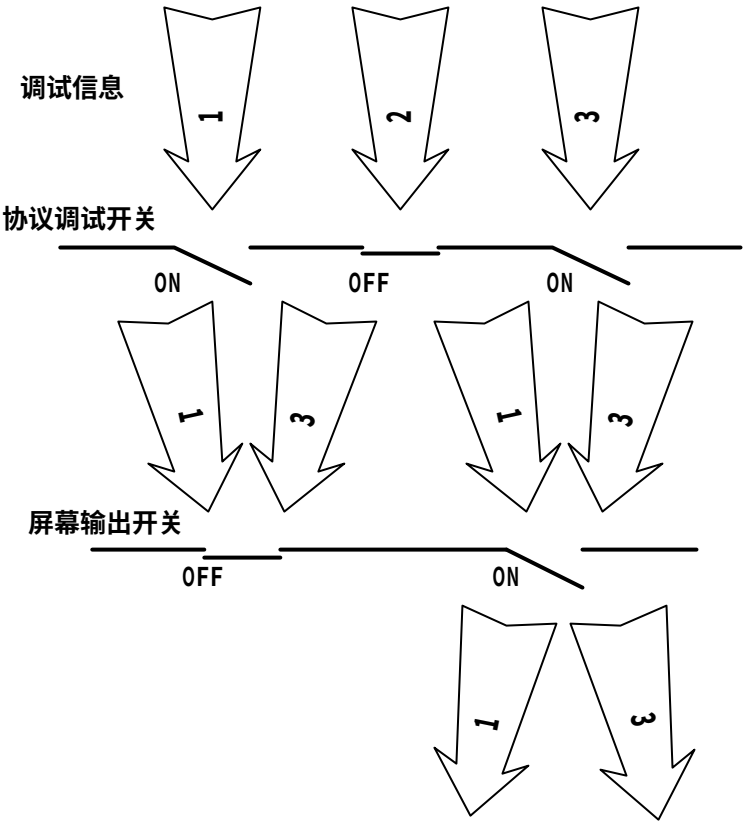


图3-1 **调试信息输出示意图**

对上述两种开关的操作参见下表。

表3-10 **调试开关的打开和关闭**

操作	命令
打开协议调试开关	**debug** { **all** | *moduname* [*debug-option*] }
关闭协议调试开关	**no debug** { **all** | { *protocol-name* | *function-name* } [*debug-option*] }
打开屏幕输出开关	**terminal debugging**
关闭屏幕输出开关	**no 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 debug all 命令，在调试结束后，应关闭全部调试开关.

第4章 SNMP 配置

4.1 SNMP 协议介绍

目前，计算机网络中用得最广泛的网络管理协议是简单网络管理协议（Simple Network Management Protocol，简称 SNMP），是被广泛接受并投入使用的工业标准，它的目标是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、进行修改、寻找故障，并完成故障诊断、容量规划和报告生成。它采用轮询机制，提供最基本的功能集，最适合小型、快速和低价格的环境使用。它只要求无证实的传输层协议 UDP，得到许多产品的广泛支持。

SNMP 的结构分为 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，根据报文类型对管理变量进行 Read 或 Write 操作，并生成 Response 报文，返回 NMS。另一方面，Agent 在设备发生冷/热启动等异常情况时，也会主动向 NMS 发送 Trap 报文报告所发生的事件。

4.2 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，就象一棵树，树的节点表示管理对象，如图 4-1 所示，它可以用从根开始的一条路径别无二义地识别。

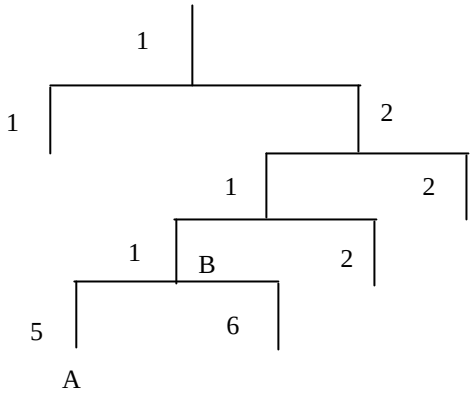


图4-1 MIB 树结构

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）。而 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。

目前 S2000 系列以太网交换机中的 SNMP Agent 支持 SNMP V3，支持的 MIB 如下表所示。

表4-1 S2000 系列以太网交换机支持的 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	

4.3 SNMP 配置

4.3.1 SNMP 的主要配置任务列表

SNMP 的主要配置任务列表如下：

- 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

4.3.2 设置团体名

SNMP V3 采用团体名认证方案，与设备认可的团体名不符的 SNMP 报文将被丢弃。SNMP 团体（Community）由一字符串来命名，称为团体名（Community Name）。不同的团体可具有只读（read-only）或读写（read-write）访问模式。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。

请在全局配置模式下进行下列配置。

表4-2 设置团体名

操作	命令
设置团体名及访问权限	**snmp-server community** *community-name* [**view** *view-name*] [**ro** | **rw**]
取消团体名及访问权限	**no snmp-server community** *community-name*

4.3.3 设置管理员的标识及联系方法

sysContact 是 MIB II 中 system 组的一个管理变量，内容为被管理设备（S2000）相关人员的标识及联系方法。

请在全局配置模式下进行下列配置。

表4-3 **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-server contact** *sysContact*
恢复管理员的标识及联系方法为缺省值	**no snmp-server contact**

4.3.4 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。**

请在全局配置模式下进行下列配置。

表4-4 **允许或禁止发送** Trap

操作	命令
允许发送 Trap	**snmp-server enable traps** [**snmp** [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]]
禁止发送 Trap	**no snmp-server enable traps** [**snmp** [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]]

4.3.5 设置 Trap 目标主机的地址

该配置任务用来设置或删除发送 Trap **信息的目标主机的** IP **地址。**

请在全局配置模式下进行下列配置。

表4-5 **设置** Trap **目标主机的地址**

操作	命令
设置 Trap **目标主机地址**	**snmp-server host** *host-ip-address* [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** } } | **udp-port** *udp-port-number*] *community-name*
删除 Trap **目标主机地址**	**no snmp-server host** *host-ip-address community-name*

4.3.6 设置 S2000 系列以太网交换机位置

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。

请在全局配置模式下进行下列配置。

表4-6 设置以太网交换机位置

操作	命令
设置以太网交换机位置	**snmp-server location** *sysLocation*
恢复以太网交换机位置的缺省设置	**no snmp-server location**

缺省情况下 *sysLocation* 为“Beijing China”。

4.3.7 设置本地或远端设备的名字

该配置任务用来设置本地或远端设备的引擎 ID，缺省为公司的企业号+设备信息，设备信息可以是 IP 地址、MAC 地址或自己定义的文本。

请在全局配置模式下进行下列配置。

表4-7 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-server engineid** *engineid*
设置设备的引擎 ID 为缺省值	**no snmp-server engineid** *engineid*

4.3.8 设置或删除一个 SNMP 的组

该配置任务用来设置或删除 SNMP 的一个组。

请在全局配置模式下进行下列配置。

表4-8 设置或删除一个 SNMP 组

操作	命令
设置一个 SNMP 组	**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]
删除一个 SNMP 组	**no snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

4.3.9 指定发送 Trap 的源地址

该配置任务用来设定或取消发送 Trap 的源地址。

请在全局配置模式下进行下列配置。

表4-9 设定发送 Trap 的源地址

操作	命令
指定发送 Trap 的源地址	**snmp-server trap-source vlan-interface** *vlan_id*
取消发送 Trap 的源地址	**no snmp-server trap-source**

4.3.10 SNMP 组添加一个新用户或删除一个用户

该配置任务用来为 SNMP 组添加或删除一个用户。

请在全局配置模式下进行下列配置。

表4-10 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-server user** *username groupname* { **v1** | **v2c** | **v3** [**auth** { **md5** | **sha** } *authpassword* [**priv des56** *privpassword*]]}
删除 SNMP 组的一个用户	**no snmp-server user** *username groupname* { **v1** | **v2c** | **v3** }

4.3.11 创建或更新视图的信息或删除视图

该配置任务用来创建、更新视图的信息或删除视图。

请在全局配置模式下进行下列配置。

表4-11 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-server view** *view-name oid-tree* { **included** | **excluded** }
删除视图	**no snmp-server view** *view-name*

4.3.12 设置 Agent 能接收/发送的 SNMP 消息包的大小

该配置任务用来设置 Agent 能接收/发送的 SNMP 消息包的大小。

请在全局配置模式下进行下列配置。

表4-12 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-server packetsize** *byte-count*
恢复 SNMP 消息包的大小的缺省值	**no snmp-server packetsize**

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。

4.3.13 SNMP 监控和维护

请在特权用户模式下进行下列操作。Show 命令可以在除普通用户模式外的所有模式下使用。

表4-13 SNMP 的监控与维护

操作	命令
显示 SNMP 报文统计信息	**show snmp**
显示当前设备的引擎 ID	**show snmp engineid**
显示路由器上的组名、安全模式、各种视图的状态以及各组存储方式的信息。	**show snmp group**
显示组用户名表中所有 SNMP 用户名称的信息	**show snmp user**
显示当前配置的团体名	**show snmp community**
显示当前配置的 MIB 视图	**show snmp view**
显示系统联络字符串	**show snmp contact**
显示系统位置字符串	**show snmp location**
打开 SNMP 调试开关	**debug snmp** { **headers** | **packets** | **trap** | **process** }

show snmp 命令输出 SNMP Agent 收发报文的统计数字。

Quidway# show snmp

```
70 SNMP packets input.
```

```
0 Bad SNMP version errors
0 Unknown community name.
0 Illegal operation for community name supplied.
0 Encoding errors.
0 Number of requested variables
0 Number of altered variables
10 Get-request PDUs.
60 Get-next PDUs.
0 Set-request PDUs.
73 SNMP packets output.
0 Too big errors. (Maximum packet size 1500)
4 No such name errors.
0 Bad values errors.
0 General errors.
0 Response PDUs
3 SNMP trap PDUs.
```

以上显示信息的含义如下表所示：

表4-14 SNMP **报文统计信息**

显示信息	意义
Unknown community name	**不能识别的团体名**
Illegal operation for community name supplied	**非法操作**
Encoding errors	**编码错误**
Get-request PDUs	Get-request **报文**
Get-next PDUs	Get-next **报文**
Set-request PDUs	Set-request**报文**
Too big errors	**响应报文太大，无法产生响应报文**
No such name errors	**不存在指定实例**
Bad values errors	**设定值类型错误**
General errors	**一般性错误**
Get-response PDUs	Get-response**报文**
SNMP trap PDUs	SNMP trap **报文**

4.4 SNMP**配置举例**

1. **组网需求**

以下图为例，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。

2. **组网图**

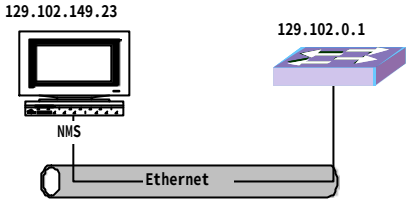


图4-2 SNMP **配置举例组网图**

3. **配置步骤**

！**进入全局配置模式。**

Quidway> enable

password:

Quidway# config

Configuring from terminal [terminal]?

此时敲回车，或者 terminal **就可进入全局配置模式，提示如下：**

Enter configuration commands, one per line. End with CTRL/z

！**设置团体名和访问权限。**

Quidway(config)# snmp-server community public ro

Quidway(config)# snmp-server community private rw

！**设置管理员标识、联系方法以及以太网交换机物理位置。**

Quidway(config)# snmp-server contact Mr.Wang-Tel:3306

Quidway(config)# snmp-server location telephone-closet,3rd-floor

！**允许发送** Trap**。**

Quidway(config)# snmp-server enable traps

4. **配置** NMS

Quidway S2000 **系列以太网交换机 支持华为公司的** iManager N2000 **及** iManager Quidview **网管系统。用户可利用网管系统完成对** S2000 **系列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5章 RMON 配置

5.1 RMON 简介

RMON（Remote Monitoring，远程监视）是 IETF 定义的一种 MIB，是对 MIB II 标准最重要的增强，主要实现对一个网段乃至整个网络中数据流量的监视功能，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），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，对其端口所连接的网段上的各种流量信息进行跟踪统计，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。它使 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。这种方法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：

- 一种方法是通过专用的 RMON probe（探测仪）。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。NMS 用 SNMP 的基本命令与其交换数据信息，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。

目前 S2000 系列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，从而实现对网络（往往是远程的）的管理。

RMON 的另一个重要的优点在于它与现存的 SNMP 框架相兼容，不需对该协议进行任何修改。

5.2 RMON 配置

5.2.1 RMON 配置任务列表

RMON 配置任务列表如下：

- 在报警表中添加/删除一行
- 在事件表中添加/删除一行
- 在历史控制表中添加/删除一行
- 在统计表中添加/删除一行

5.2.2 在报警表中添加/删除一行

RMON 报警管理可对指定的报警变量（如端口的统计数据）进行监视，当被监视数据的值越过定义的阈值时会产生报警事件，事件通常会记录在设备的日志表中，并向 NMS 发送 Trap 消息。事件的定义在事件管理中实现。报警管理的功能包括：报警项的浏览、增加及删除。

请在全局配置模式下进行下列配置。

表5-1 在报警表中添加/删除一行

操作	命令
在报警表中添加一行信息	**rmon alarm** *entry_number alarm_variable sampling_time* { **delta** | **absolute** } **rising-threshold** *threshold_value1* [*event_entry1*] **falling-threshold** *threshold_value2* [*event_entry2*] [**owner** *text*]
在报警表中删除一行信息	**no rmon alarm** *entry_number*

5.2.3 在事件表中添加/删除一行

RMON 的事件管理定义事件号及事件的处理方式——记日志、向网管站发 Trap 消息、或者记日志同时向网管站发 Trap 消息。

请在全局配置模式下进行下列配置。

表5-2 在事件表中添加/删除一行

操作	命令
在事件表中添加一行	**rmon event** *event_entry* [**description** *string*] { **log** | **trap** *trap_community* | **log-and-trap** *log_trapcommunity* } [**owner** *rmon_station*]
在事件表中删除一行	**no rmon event** *event_entry*

5.2.4 在历史控制表中添加/删除一行

历史数据管理功能可以对设备设置历史数据采集任务，定期对指定的端口进行数据采集并保存起来以备查看。抽样信息包括利用率、错误数和总包数等。

请在全局配置模式下进行下列配置。

表5-3 在历史控制表中添加/删除一行

操作	命令
在历史控制表中添加一行	**rmon history** *entry_number port_num* **buckets** *number* **interval** *sampling_interval* [**owner** *text_string*]
在历史控制表中删除一行	**no rmon history** *entry_number*

5.2.5 在统计表中添加/删除一行

RMON 统计管理可以设置对监视端口的使用及错误进行统计。统计信息包括冲突、循环冗余校验和队列、太小或超大包、超时传送、碎片、广播、多播、单播消息以及带宽使用等。

请在全局配置模式下进行下列配置。

表5-4 在统计表中添加/删除一行

操作	命令
在统计表中添加一行	**rmon statistics** *entry_number port_num* [**owner** *text_string*]
在统计表中删除一行	**no rmon statistics** *entry_number*

5.3 RMON 监控与维护

请在除普通用户模式外的所有配置模式下进行下列操作。其中 show 命令还可在除普通用户模式外的所有模式下进行。

表5-5 RMON 监控与维护

操作	命令
显示 RMON 统计消息	**show rmon statistics** [port_num]
显示 RMON 历史信息	**show rmon history** [*port_num*]
显示 RMON 告警信息	**show rmon alarm** [*alarm_table_entry*]
显示 RMON 事件	**show rmon event** [*event_table_entry*]
显示 RMON 事件日志	**show rmon eventlog** [*event_number*]
打开 RMON 调试开关	**debug rmon**
关闭 RMON 调试开关	**no debug rmon**

(1) 显示 RMON统计表消息

Quidway# show rmon statistics

```
Interface Ethernet0/1, with ethernet statistics table index 1, is VALID,
  and owned by Configer.
  It has Received 22364 octets, 233 packets,
  121 broadcast and 110 multicast packets,
  0 undersized and 0 oversized packets,
  0 fragments and 0 jabbers,
  0 CRC alignment errors and 0 collisions.
  Dropped packet events (due to lack of resources): 0.
  Packets received of length (in octets):
  64: 120, 65-127: 88, 128-255: 8,
  256-511: 12, 512-1023: 5, 1024-1518: 0.
```

以上信息表示：用户端口号为 Ethernet0/1，**行索引为** 1，**行创建者为** Configer，**总字节数为** 22364，**总包数为** 233，**广播包数**（broadcast）**为** 121，**多播包数**（multicast packets）**为** 110，**过小包数**（undersized）、**超大包数**（oversized packets）、**过小又校验出错的包**（fragments）、**过大又校验出粗的包**（jabbers）、**校验出错的包**（CRC alignment errors）、**冲突的包**（collisions）、**丢包事件数**（Dropped packet events）**均为** 0，64 **字节包数为** 120，65-127 **字节包数为** 88，128-255 **字节包数为** 8，256-511 **字节包数为** 12，512-1023 **字节包数为** 5，1024-1518 **字节包数为** 0。

(2) 显示 RMON历史信息

Quidway# show rmon history

```
Interface Ethernet0/1, with history control table index 1, is VALID,
  and owned by HUAWEI.
  It has 10 buckets, sampling interval is 10.

  It's latest sampled values:
  0 dropevents and 0 octets,
  0 packets and 0 broadcastpackets,
  0 multicastpackets and 0 CRC alignment errors,
  0 undersized and 0 oversized packets,
  0 fragments and 0 jabbers,
  0 collisions and utilization is 0.
```

以上信息表示：数据源 用户端口号为 Ethernet0/1，控制行索引为 1，控制行创建者为 HUAWEI，最多可以记录 10 条记录（buckets），采样时间间隔为 10s，最近一次采样数据：丢包事件数（droppevents）、采样时间内接收字节数和包数为 0，广播包数（broadcastpackets）、多播包数（multicastpackets）、校验出错的包（CRC alignment errors）、过小包数（undersized）、超大包数（oversized packets）、过小又校验出错的包（fragments）、过大又校验出粗的包（jabbers）、冲突的包（collisions）、利用率（utilization）均为 0，。

(3) 显示 RMON 告警信息

Quidway# show rmon alarm

```
Alarm table 1 is UNDERCREATION, and owned by Configer,
  every 1 second(s) monitoring Ethernet0/1 ebcastpkts.
  Rising threshold is 2, linked with event 5.
  Falling threshold is 1, linked with event 5.
  On startup enables risingOrFallingAlarm.
  Its latest absolute sampled values was 0.
```

以上信息表示：报警表中 1 号事件是无效的（UNDERCREATION），所有者是 Configer，每隔 1 秒对端口 Ethernet0/1 接收和发送的广播包数（ebcastpkts）进行一次监测，上限阈值（Rising threshold）为 2 将会引发 5 号事件，下限阈值（Falling threshold）为 1 将会引发 5 号事件，超过上限阈值或低于下限阈值将会引发告警信息，最近一次绝对采样值为 0。

(4) 显示 RMON 事件

Quidway# show rmon event

```
Event table 1 is VALID, and owned by HUAWEI.
  Description: none.
  Event firing causes log ,last fired at 0.
```

以上信息表示：事件表中 1 号事件是有效的，所有者是 HUAWEI，对事件无描述，事件引发日志，最近一次事件发生的时间是 0 时刻（此时间是以系统初始化/启动以来的厘秒数计算的）。

(5) 显示 RMON 事件日志

Quidway# show rmon eventlog 1

```
Event table 1 is VALID, and owned by huawei.
  Description: none.
  Event firing causes log-and-trap ,last fired at 102300.

Event 1 generates eventLog 1.
 Description: The 1.3.6.1.2.1.16.1.1.1.4.8 defined in alarm table 2,
     less than 200 with alarm value 0. Alarm sample type is delta.
    loged at 21300.

Event 1 generates eventLog 2.
 Description: The 1.3.6.1.2.1.16.1.1.1.4.8 defined in alarm table 2,
     uprise 1000 with alarm value 10443. Alarm sample type is delta.
    loged at 102300.
```

以上信息表示（仅以第一段为例）：事件表中 1 号事件是有效的，事件的所有者是 huawei，对事件没有描述，事件引发日志和告警，最近一次事件发生在时刻 102300（此时间是以系统初始化/启动以来的厘秒数计算的）。

5.4 RMON 配置举例

1. 组网需求

此配置示例在 RMON 以太网统计表中设定一行，进行以太网端口性能统计，以便网管查询。

2. 组网图

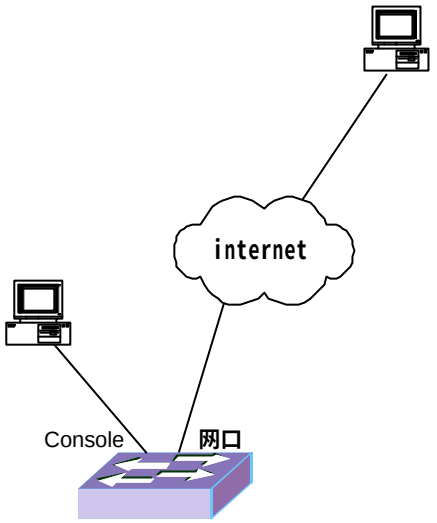


图5-1 配置 RMON 组网图

3. 配置步骤

！配置 RMON。

Quidway(config)# rmon statistics 1 ethernet 0/8 owner huawei_rmon

！在特权用户模式下查看配置。

Quidway# show rmon statistics ethernet 0/8

```
Interface Ethernet0/8, with ethernet statistics table index 1, is VALID,
and owned by huawei_rmon.
It has Received 270149 octets, 1954 packets,
1570 broadcast and 365 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
Dropped packet events (due to lack of resources): 0.
Packets received of length (in octets):
```

```
64: 644, 65-127: 518, 128-255: 688,
256-511: 101, 512-1023: 3, 1024-1518: 0.
```