目 录

第1章 系统管理概述

用户在了解本手册的第一个模块《入门》的基础上，为了对路由器进行进一步的管理和维护，保障路由器的正常运行，有必要掌握本模块《系统管理》的内容。

系统管理的文档组织如下：

- 系统维护管理
- 文件管理
- 用户界面（User-interface）管理
- 用户管理
- NTP（Network Time Protocol）配置
- SNMP（Simple Network Management Protocol）配置
- 终端服务

1. 系统维护管理

系统维护管理介绍了 VRP 提供方便的系统调试和维护工具以及信息中心的功能，这为网络管理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。

2. 文件管理

文件管理介绍了 VRP 所支持的文件系统功能，用户通过文件系统可以管理设备的硬盘和 Flash Memory 中的文件，包括主机软件、配置文件、日志文件等。

文件管理还介绍了 FTP 协议、TFTP 协议，通过这些协议，用户可以在路由器和其他设备之间进行文件传输。

3. 用户界面管理

用户界面管理介绍了 VRP 支持的 4 种用户界面，即 Console（CON）口、Auxiliary（AUX）口、异步方式串口（TTY）、虚拟线路（VTY）等。VRP 提供了用户界面视图，用来管理这 4 种用户界面，控制用户通过这些接口对路由器的访问。

4. 用户管理

用户管理介绍了 VRP 实现的用户管理策略，通过这些措施，路由器的系统管理员可以方便有效地管理用户及其所使用的服务，增强网络的安全性。

5. NTP 配置

NTP 配置介绍了 NTP 以及 NTP 的配置，VRP 提供的 NTP 服务可以使系统与其他支持 NTP 的设备一起，保证网络内各设备的时间一致，保证互操作的可靠性。

6. SNMP 配置

SNMP 配置介绍了 SNMP 及其配置，SNMP 与网络管理系统一起对网络中运行的设备进行有效管理。

7. BIMS

BIMS 分 BIMS 中心侧和 BIMS 设备侧两个部分，其基本原理是：设备侧启动中或启动以后按照某种策略定期或间隔一定的时间向 BIMS 中心发出特定的信息请求，BIMS 中心侧根据管理员下达的策略指示同设备进行信息交互。在中心侧和设备侧的信息交互过程中，管理员可以对设备进行管理，执行诸如升级软件版本、更改配置、查看配置信息和状态信息等任务，从而达到管理员对设备实施集中管理的功能。

8. RMON

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 MIB 由一组统计数据、分析数据和诊断数据组成。不像标准 MIB 仅提供被管理对象大量的关于端口的原始数据，它提供的是一个网段的统计数据和计算结果。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。

9. 终端服务

终端服务介绍了 VRP 提供各种终端服务功能，主要包括 Console 口终端服务、AUX 口的终端服务、Telnet 终端服务、SSH 终端服务、PAD 终端服务、哑终端服务等，用户既可以在本地对设备进行管理，也可以通过网络对设备进行远程管理，而不必为每一台设备连接一个物理终端。

第2章 系统维护管理

系统维护管理主要包括以下几项内容：

- 系统维护调试工具的使用
- 系统信息中心的维护管理

2.1 auto-config 功能

2.1.1 auto-config 功能简介

auto-config 功能是一项能够对初次安装使用的路由器进行自动检测、自动配置的便捷功能。它能够在不需要用户干预的情况下自动检测并配置所有的 serial 口、E1/T1/E3/T3 接口、以太网接口、AM 接口，然后运行 telnet、ftp、web 等服务，通过预先配置好网络中心设备（路由器或配置终端）自动完成对外围路由器的控制，如进行配置管理或者把预先准备好的配置文件下载给外围路由器。该功能主要用于企业网末端的中低端路由器，可以针对待配置路由器上提供的具体接口类型来搭建自动远程配置网络：

- 对于 E1、T1、E3、T3 接口，一般采用 PDH/SDH 网络的光纤传输线路连接待配置路由器与中心路由器。
- 对于 Serial（同步模式）、Async、E1-F、T1-F 接口，一般可采用 DDN 网络提供的同/异步专线连接待配置路由器与中心路由器。
- 对于 10/100M Ethernet 接口采用 10/100M 以太网连接待配置路由器与中心路由器。
- 对于 AM（AnalogModem）接口，应通过 PSTN 提供的模拟电话线以流方式拨号连接待配置路由器与远程配置终端。

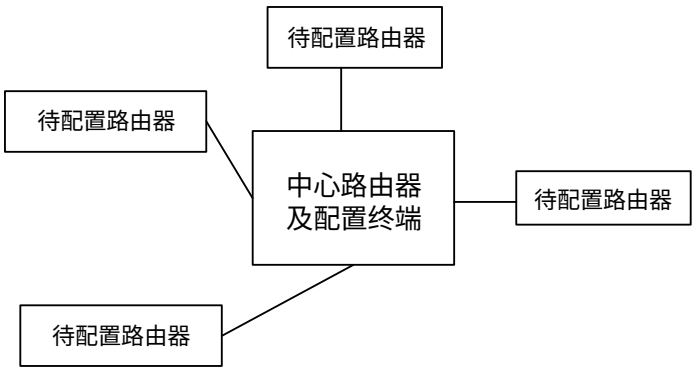

图2-1 auto-config 功能组网应用示意图

在路由器启动过程中通过检测配置文件决定是否执行 auto-config 功能，具体实现流程如下：

(1) 如果检测到配置文件，则直接运行配置文件，不执行 auto-config 功能。

(2) 如果没有配置文件，检测到出厂缺省配置文件（vrpcfg .def），则执行出厂缺省配置文件，不执行 auto-config 功能。

(3) 如果没有检测到以上配置文件，则自动运行 **auto-config** 命令（缺省情况下 auto-config 使能标志为 enable），执行如下批处理：

- 对于 Serial 接口，在接口上封装 PPP 链路协议，所有 Serial 接口工作在 PPP Negotiate 方式下，指定缺省的用户名和口令，支持 telnet、ftp 等服务。
- 对于 Controller（e1/e3/t3）接口，使用 **using** { **e1**| **t3** | **e3** }命令，生成对应的 serial 接口，并完成与 Serial 接口相同的配置；对于 Controller（t1）接口，通过 channel-set 命令将所有时隙捆绑成一个串口，并完成与 Serial 接口相同的配置。
- 对于 Ethernet 接口，启动 dhcp client 等待对端分配地址，指定缺省的用户名和口令，支持 telnet、ftp 等服务。
- 对于 AM 接口，配置工作方式为流方式，设置 modem 的编码格式，并支持 terminal 服务。

📖 说明：

有关配置文件启动顺序的详细说明，请参见“ 配置文件管理 ”部分。

2.1.2 在待配置路由器上手工配置 auto-config 功能

1. 使能 auto-config 功能

请在系统视图下进行下面配置。

表2-1 使能/关闭 auto-config 功能

操作	命令
使能 auto-config 功能	**auto-config enable**
关闭 auto-config 功能	**undo auto-config**

缺省情况下为 **enable。**

2. 执行 auto-config 操作

⚠ 注意：

由于 **auto-config** 命令相当于执行一系列实际命令的批处理，即该命令会改变用户的当前配置，且不提供 **undo** 命令来取消上次的操作，故该命令一般在初次启动路由器时使用，在已经完成了配置的组网环境下请务必谨慎使用！

auto-config 命令不能被保存（save），但出厂缺省配置文件 vrpcfg .def 中可以提供 auto-config 功能。

请在系统视图下进行下面配置。

表2-2 执行 auto-config 操作

操作	命令
启动 auto-config 功能	**auto-config**

执行 **auto-config** 操作相当于执行一系列命令的批处理，具体命令如下：

(1) 启动 ftp 功能， 配置 VTY（telnet）、TTY（通过 AM 接口连接的拨号用户）用户采用本地认证。

```
ftp server enable
user-interface vty 0 4
authentication-mode scheme
user-interface tty user-interface-number
modem call-in
speed 57600
authentication-mode scheme
```

(2) 配置本地认证缺省的用户名和密码，并为缺省用户提供 telnet、ftp、terminal 等服务。

```
local-user admin password cipher admin
level 3
service-type ftp
service-type terminal telnet
```

缺省的用户名和口令都是 admin。

(3) 检测所有的 Controller 接口，对 E1/E3/T3 接口设定工作状态为非通道化，生成对应的 Serial 口；对于 T1 接口通过 channel-set 命令将所有时隙捆绑成一个 Serial 口。

```
controller e1 interface-number
using e1
controller e3 interface-number
```

```
using e3
controller t3 interface-number
using t3
controller t1 interface-number
channel-set 0 timeslot-list 1-24
```

(4) 检测所有的 serial 接口（包括 Controller 生成的逻辑接口），封装链路层协议为 PPP，配置 IP 地址为 PPP 地址协商，将接口置为 **UP** 状态。

```
Interface serial interface-number
link-protocol ppp
ip address ppp-negotiate
undo shutdown
```

(5) 检测所有的 Ethernet 接口，启动 dhcp client 功能，将接口置为 **UP** 状态。

```
Interface ethernet interface-number
ip address dhcp-alloc
undo shutdown
```

(6) 检测所有的 AM 接口，配置工作方式为流方式，配置 Modem 编码格式（若设备上有 E1/E3 模块，则设置 CountryCode 为 UK，否则 CountryCode 均为 US），将接口置为 **UP** 状态。

```
Interface analogmodem interface-number
async mode flow
country-code { united-kingdom | united-states }
undo shutdown
```

2.1.3 配置中心路由器

中心路由器或配置终端需要由网络管理员完成配置，管理员可以根据网络连接情况确认需要配置哪些接口。下面对各种接口及相关配置分别进行说明：

1. 串口（Serial/Async/E1-F/T1-F 接口）相关配置

📖 说明：

Serial/Async/E1-F/T1-F 接口配置相似，都是封装 PPP 协议，并为对端分配 IP 地址；不同的是 Serial/E1-F/T1-F 接口的工作模式为同步模式（即缺省设置），并在 serial 视图下进行下面配置，而 Async 接口为异步模式，并在 Async 接口视图下进行下面配置。

---

(1) 配置 IP 地址池

请在系统视图下进行下列配置。

表2-3 配置 IP 地址池

操作	命令
定义为 PPP 用户分配地址的 IP 地址池	**ip pool** *pool-number*

(2) 在串口上封装 PPP 链路协议

请在串口视图下进行下面配置。

表2-4 在串口上封装 PPP 链路协议

操作	命令
在串口上封装 PPP 链路协议	**link-protocol ppp**

(3) 在串口上为对端分配 IP 地址

请在串口视图下进行下列配置。

表2-5 配置为对端分配 IP 地址

操作	命令
配置为对端接口分配 IP 地址	**remote address** { *ip-address* | **pool** [*pool-number*] }

2. E1/T1/E3/T3 接口相关配置

请在 Controller e1/t1/e3/t3 接口视图下进行下列配置。

表2-6 配置 E1/T1/E3/T3 接口工作状态

操作	命令
配置 E1 接口工作状态为非通道化	**using e1**
配置 T1 接口所有时隙捆绑成串口	**channel-set 0 timeslot-list 1-24**
配置 E3 接口工作状态为非通道化	**using e3**
配置 T3 接口工作状态为非通道化	**using t3**

另外，还要在生成的对应 serial 接口上完成同上面串口相同配置。

3. 以太网接口相关配置

启动 DHCP Server 为待配置路由器对应的 Ethernet 接口分配 IP 地址

表2-7 创建 DHCP 地址池并配置动态分配的 IP 地址范围

操作	命令
创建 DHCP 地址池或进入 DHCP 地址池视图（系统视图）	**dhcp server ip-pool** *pool-name*
配置动态分配的 IP 地址范围（DHCP 地址池视图）	**network** *ip-address* [**mask** *netmask*]

4. 发起 Telnet/FTP 连接

首先应确认待配置路由器的接口 IP 地址，然后发起 Telnet/FTP 连接登录到路由器进行配置或加载配置文件。

Telnet/FTP 登录时，缺省使用的用户名和口令都是 admin。

5. 通过 AM 接口进行拨号连接

首先待配置路由器的 AM 接口已经通过 PSTN 连接到中心机房的远程配置终端上，此时配置管理员即可在远程终端上通过终端仿真程序（如 Windows 的 Hyperterm（超级终端））以流方式向路由器拨号，与路由器建立连接。在终端仿真程序中选择实际连接时使用的 RS-232 串口，设置终端通信参数为 9600 波特率、8 位数据位、1 位停止位、无奇偶校验、无流量控制或硬件流量控制，并选择终端仿真类型为 VT100 或自动检测。

拨号登录时，缺省使用的用户名和口令都是 admin。

🕮 说明：

以上列出的为关键配置，其余采用缺省配置即可。

2.1.4 auto-config 的显示和调试

请在用户视图下进行下列配置。

表2-8 auto-config 的显示和调试

操作	命令
查看 auto-config 功能的状态。	**display auto-config**

2.1.5 auto-config 典型配置举例 1

1. 组网需求

待配置路由器 R2 支持 auto-config 功能，安装了一块 1E1 接口模块。中心路由器 R1 与在待配置路由器 R2 通过 E1 口相连，管理员在 R1 上进行相应的配置，然后通过 FTP 将配置文件 quidwayR2.cfg 加载到 R2。

2. 组网图

图2-2 auto-config 典型配置举例（R2 通过 E1 口连接 R1）

3. 配置步骤

(1) 配置中心路由器 R1

配置 controller 接口。

```
[Quidway] controller e1 0/0/0
[Quidway-e1 0/0/0] using e1
```

配置 e1 接口生成的 serial0/0/0 接口，并为对端分配 IP 地址。

```
[Quidway] ip pool 1 192.10.1.1
[Quidway] interface serial0/0/0
[Quidway-serial0/0/0] link-protocol ppp
[Quidway-serial0/0/0] ip address 192.10.1.2 255.255.255.0
[Quidway-serial0/0/0] remote address pool 1
```

通过 FTP 给远端路由器加载配置文件。

```
<Quidway > ftp 192.10.1.1
[ftp] put quidwayR2.cfg vrpcfg.cfg
```

vrpcfg.cfg 为路由器上缺省的配置文件名。

(2) 待配置路由器 R2

R2 开机后自动运行 auto-config 功能，生成如下配置：

```
ftp server enable
local-user admin password cipher admin
service-type telnet terminal
level 3
service-type ftp
controller e1 0/0/0
using e1
interface serial 0/0/0
link-protocol ppp
ip address ppp-negotiate
user-interface vty 0 4
authentication-mode scheme
```

路由器上的固定接口也会同时自动生成相关配置，这里不再赘述。

2.1.6 auto-config 典型配置举例 2

1. 组网需求

待配置路由器 R2 提供一个固定以太网接口，支持 auto-config 功能。中心路由器 R1 与在待配置路由器 R2 通过以太网相连，管理员在 R1 上进行相应的配置，然后通过 FTP 将配置文件 quidwayR2.cfg 加载到 R2。

2. 组网图

图2-3 auto-config 典型配置举例（R2 通过以太网连接 R1）

3. 配置步骤

(1) 配置中心路由器 R1

配置地址池及接口 IP 地址。

```
[Quidway] dhcp server ip-pool 0
[Quidway- dhcp-0] network 192.10.1.0 mask 255.255.255.0
[Quidway- dhcp-0] quit
[Quidway] interface ethernet0/0/0
[Quidway-ethernet0/0/0] ip address 192.10.1.2 255.255.255.0
```

通过 FTP 给远端路由器加载配置文件。

```
<Quidway > ftp 192.10.1.1
[ftp] put quidwayR2.cfg vrpcfg.cfg
```

通过 display dhcp server ip-in-use 命令可以查看到分配给 R2 的地址为 192.10.1.1，故直接通过 FTP 登录。vrpcfg.cfg 为路由器上缺省的配置文件名。

(2) 待配置路由器 R2

R2 开机后自动运行 auto-config 功能，生成如下配置：

```
ftp server enable
local-user admin password cipher admin
service-type telnet terminal
level 3
service-type ftp
interface ethernet 0/0/0
ip address dhcp-alloc
user-interface vty 0 4
authentication-mode scheme
```

路由器上的固定接口也会同时自动生成相关配置，这里不再赘述。

2.1.7 auto-config 典型配置举例 3

1. 组网需求

待配置路由器 R2 提供 auto-config 功能，安装了一块 SIC-1AM 接口卡和一块 E1 接口模块。待配置路由器 R2 的 AM 接口通过 PSTN 与远程配置终端相连，管理员在远程配置终端上发起拨号，并登录到 R2 上进行配置。

2. 组网图

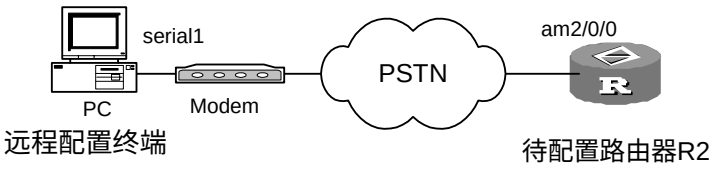

图2-4 auto-config 典型配置举例（配置终端通过 AM 口连接 R2）

3. 配置步骤

(1) 配置 R1

在远程配置终端（PC 的超级终端）上配置如下参数：

连接时使用的接口：串口 1

波特率（B）：9600

数据位（D）：8

奇偶校验（P）：无

停止位（S）：1

流量控制（F）：无或硬件

终端仿真（E）：VT100 或自动检测

建立拨号连接后即可登录到 R2。

(2) 待配置路由器 R2

R2 开机后自动运行 auto-config 功能，生成如下配置：

```
ftp server enable
local-user admin password cipher admin
service-type telnet terminal
level 3
service-type ftp
interface analogmodem 2/0/0
async mode flow
```

```
country-code united-kingdom
user-interface tty 0
modem call-in
authentication-mode scheme
```

路由器上的固定接口和 E1 接口也会同时自动生成相关配置，这里不再赘述。

2.2 系统维护与调试

2.2.1 网络连接的测试工具

1. ping

ping 主要用于检查网络连接及主机是否可达。

请在任何视图下进行操作。

表2-9 ping 命令

操作	命令
支持 IP 协议 ping	**ping** [-**a** *X.X.X.X*] [-**c** *count*] [-**d**][-**f**] [-**h** *ttl_value*] [-**i** *interface-type interface-number*][**ip**] [-**n**] [-**p** *pattern*] [-**q**] [-**r**][-**s** *packetsize*] [-**t** *timeout*] [**tos**][-**v**] [**vpn-instance** *vpn-instance-name*] *host*

各选项及参数意义详见命令手册 **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
0.00% 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。

请在任何视图下进行下列操作。

表2-10 tracert 命令

操作	命令
Trace Route	**tracert** [**-a** *X.X.X.X*] [**-f** *first_TTL*] [**-m** *max_TTL*] [**-p** *port*] [**-q** *nqueries*] [**vpn-instance** *vpn-instance-name*] [**-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。

例 1：

```
<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。

例 2：

```
<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
```

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。

2.2.2 系统调试功能

系统的命令行接口提供了种类丰富的调试功能，对于路由器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，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。

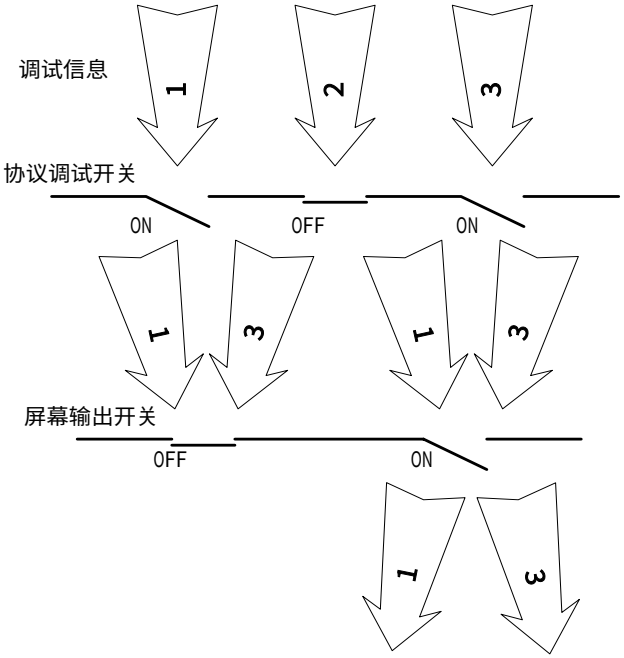

图2-5 调试信息输出示意图

协议调试开关由 **debugging** 控制，请在用户视图下进行下列配置。

表2-11 调试开关的打开、关闭和显示

操作	命令
打开协议调试开关	**debugging** { **all** | *module-name* [*debug-option1*] [*debug-option2*] …}
关闭协议调试开关	**undo debugging** { **all** | *module-name* [*debug-option1*] [*debug-option2*] … }
显示已经打开的调试开关	**display debugging** [**interface** *interface-type interface-number*] [*module-name*]

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。

屏幕输出开关由信息中心控制，详细说明参见下节。

2.2.3 配置系统重启

在路由器运行过程中，由于系统文件升级等原因，需要重启路由器。这时，您可以对路由器下电再上电，也可以使用 **reboot** 命令。

请在用户视图下进行下列配置。

表2-12 配置系统重启

操作	命令
直接重新启动路由器	**reboot**

⚠ 注意：

一般情况下，不要轻易使用该命令，因为它将导致网络工作在短时间内瘫痪，另外在重启路由器时，要确认是否需要保存路由器配置文件。

2.3 信息中心功能

2.3.1 信息中心简介

信息中心是路由器主体软件中不可或缺的一部分，它作为路由器的信息枢纽而存在。信息中心接管大多数的信息输出，并能进行细致的分类，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。

系统的信息中心具有以下一些特性：

- 信息中心共有三类信息：log 类（日志类信息）、trap 类（告警类信息）、debug 类（调试类信息）。
- 信息按重要性划分为八种等级，可按等级进行信息过滤。
- 系统支持十个通道，其中前六个通道（通道 0～通道 5）有缺省通道名，并且这六个通道缺省的与六个输出方向相关联，可以通过命令改变通道名，也可以改变通道与输出方向之间的关联。
- 支持控制台（console）、Telnet 终端和配置终端（monitor）、日志缓冲区（logbuffer）、日志主机（loghost）、告警缓冲区（trapbuffer）、SNMP 六个方向的信息输出。
- 系统由众多的协议模块、单板驱动程序、配置模块构成，信息可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。
- 每个信息的头部由固定的部分组成，包括时间戳、信息来源的模块、信息级别、信息来源的槽号、信息摘要等。

总之，信息中心的主要工作就是将各种模块的三种类型的信息，按照八种重要程度，根据用户的设置输出到十个信息通道中去，然后，将这十个信息通道再定位到六个输出方向上去。

2.3.2 信息中心配置

1. 开启/关闭信息中心的功能

请在系统视图下进行下列配置。

表2-13 开启/关闭信息中心功能

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。在信息中心开启时，特别是在处理信息较多时，由于信息分类、输出的原因，对系统性能有一定的影响。

2. 信息通道的命名

请在系统视图下进行下列配置。

表2-14 信息通道的命名

操作	命令
将编号为 channel-number 的信息通道命名为 channel-name	**info-center channel** *channel-number* **name** *channel-name*

channel-number 是通道号，取值为 0～9，即系统有 10 个通道。*channel-name* 是通道名，最长为 30 个字符，不支持“ - ”、“ / ”和“ \ ”等字符。

通道 0～5 系统指定了缺省名，如下表：

表2-15 通道的缺省名

channel-number（通道号）	channel-name（通道名）
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent

3. 信息优先级（severity）

信息中心按信息的严重等级或紧急程度将其划分为八个等级；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阈值的信息输出。越紧急的信息报文，其严重等级越小，emergencies 表示的等级为 1，debugging 为 8，因此，当设置严重等级阈值为 debugging 时，所有的信息都会输出。

表2-16 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

设置将 snmp 通道中的 IP 协议模块的日志类信息打开，且允许严重等级值小于等于 warning 级别的信息输出。

```
[Quidway] info-center source ip channel snmpagent log level warnings
```

4. 定义信息通道的内容

请在系统视图下进行下列配置。

表2-17 定义信息通道的内容

操作	命令
向信息通道中添加记录	**info-center source** { *module-name* | **default** } { **channel** { *channel-number* | *channel-name*} } [**log** { **state** { **on** | **off** } | **level** *severity* }* | **trap** { **state** { **on** | **off** } | **level** *severity* } * | **debug** { **state** { **on** | **off** } | **level** *severity* }*]*
删除信息通道中的记录	**undo info-center source** { *module-name* | **default** } { **channel** { *channel-number* | *channel-name* }

module-name 是模块名。**default** 代表信息通道中的缺省记录。**level** 设置信息级别，禁止信息级别大于所设置的 *severity* 的信息输出。*severity* 是信息级别。*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**，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。

⚠ 注意：

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，这些参数包括按模块过滤设置，中英文选择，严重等级阈值等，这些设置被某一个用户改变时，在别的用户端也有反映。

5. 信息的输出

目前，路由器主体软件的信息中心可以在 7 个方向上输出各种信息：

- 通过 Console 口向本地控制台输出信息。
- 向远程 Telnet 终端输出信息。此功能有助于远程维护。
- 在路由器内部分配适当大小的日志缓冲区，用于记录信息。
- 配置日志主机，信息中心直接将信息发往日志主机，并在其上以文件的形式保存起来，供随时查看。
- 在路由器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。
- 向日志文件输出信息

每个输出方向通过配置命令指定所需要的通道，所有信息经过通道的过滤后，再发送到相应的输出方向；可根据需要，通过配置输出方向所使用的通道以及通道的过滤信息，来完成对各类信息的过滤以及重定向。

请在系统视图下进行下列配置。

表2-18 输出信息

操作	命令
向 Console 方向输出信息	**info-center console channel** { *channel-number* | *channel-name* }
向 Telnet 终端或哑终端输出信息	**info-center monitor channel** { *channel-number* | *channel-name* }
向 SNMP 输出信息	**info-center snmp channel** { *channel-number* | *channel-name* }
设置日志缓冲区的大小，设置向日志缓冲区输出信息的通道	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **max-size** *buffersize*] *
关闭日志缓冲区或恢复默认值	**undo info-center logbuffer** [**channel** | **max-size**]
设置向日志主机输出信息的信息通道以及其它参数	**info-center loghost** *X.X.X.X* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] *

操作	命令
设置向日志文件输出日志信息的通道号	**info-center logfile channel** { *channel-number* | *channel-name* } *
取消当前设置	**undo info-center logfile channel**
取消向日志主机输出信息	**undo info-center loghost** *X.X.X.X*
设置告警缓冲区的大小，设置向告警缓冲区输出信息的通道	**info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **max-size** *buffersize*] *
关闭告警缓冲区或恢复默认值	**undo info-center trapbuffer** [**channel** | **size**]

目前，系统缺省设置了 6 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

告警缓冲区　　3　　trapbuffer

日志缓冲区　　4　　logbuffer

snmp　　5　　snmpagent

📖 说明：

六个输出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。

6. 设置发送日志信息的源地址

请在系统视图下进行下列配置。

表2-19 设置发送信息的源地址

操作	命令
设置发送信息的源地址	**info-center loghost source** *interface-type interface-number* [*subinterface-type*]
取消当前配置	**undo info-center loghost source**

2.3.3 显示终端的设置

显示终端的设置就是控制是否在用户屏幕上输出 debug/log/trap 信息，这些信息是从信息中心发送来的。

请在用户视图下进行下列配置。

表2-20 显示终端的设置

操作	命令
打开终端显示信息功能	**terminal monitor**
打开终端显示日志信息功能	**terminal logging**
打开终端显示告警信息功能	**terminal trapping**
打开终端显示调试信息功能	**terminal debugging**
关闭终端显示信息功能	**undo terminal monitor**
关闭终端显示日志信息功能	**undo terminal logging**
关闭终端显示告警信息功能	**undo terminal trapping**
关闭终端显示调试信息功能	**undo terminal debugging**

此命令只影响输入命令的当前终端的显示。

在 **undo terminal monitor**（显示终端关闭）的情况下，相当于执行 **undo terminal debugging**，**undo terminal logging**，**undo terminal trapping** 命令，所有的调试/日志/告警信息在本终端都不显示；在 **terminal monitor** 为打开的情况下，可以分别使用 **terminal debugging/undo terminal debugging**，**terminal logging/undo terminal logging**，**terminal trapping/undo terminal trapping** 打开或关闭调试/日志/告警信息。

2.3.4 syslog 功能简介

syslog 功能是通过信息中心模块（info-center）实现的，它是信息中心模块所具有的一个子功能。本小节主要对输出到日志主机的日志格式做简略的说明。输出到日志主机采用端口号 514。

本格式根据 RFC3164（The BSD syslog Protocol）制定，并对消息头部进行扩展。

日志信息格式如下：

<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，就是表 2-16中所给出的值。

优先级与时间戳之间没有任何字符。

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

该字段表示日志是由哪个模块产生的，目前产生各模块的列表如下：

表2-21 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）
CHAP	CHAP 验证（PPP 协议使用的一种验证方式）
DCC	拨号控制中心（Dial Control Center）

模块名	说明
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）
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

模块名	说明
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	虚拟用户终端（Virtual Port）

模块名与级别之间以一个斜杠(/)隔开。

5. 级别

日志的级别共分为 8 级，从 1～8，它们的定义和说明见表 2-16。

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。

7. 日志主机的设置

系统最多可设置 4 个日志主机，默认情况下，发向日志主机的日志通过通道 loghost（通道号为 2）发出，设置日志主机的命令为 **info-center loghost**。

可以设置日志的源 IP 地址为一固定接口的地址，通过这个功能可以使日志主机通过源地址来进行日志的归类管理。例如可用命令 **info-center loghost source** *loopback0* 设置系统所发出的日志源地址都为 *loopback0* 接口的地址。

2.3.5 信息中心显示与调试

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

在用户视图下，执行 **debugging** 命令可对信息中心进行调试。

表2-22 信息中心显示与调试

操作	命令
显示信息中心记录的信息	**display info-center**
显示日志缓冲区记录的信息	**display logbuffer** [**size** *size-value* | **summary**] [**level** *level-number*] [**|** [**begin** | **include** | **exclude**] *string*]
显示信息通道的内容	**display channel** [*channel-number* | *channel-name*]
显示告警缓冲区记录的信息	**display trapbuffer**

2.3.6 信息中心配置举例

1. 控制台信息输出配置举例

(1) 开启信息系统。

```
[Quidway] info-center enable
```

(2) 配置控制台日志输出，允许 PPP 模块的日志输出，严重等级限制为 emergencies～debugging。

```
[Quidway] info-center console channel console
[Quidway] info-center source ppp channel console log level debugging
```

(3) 打开 PPP 模块的调试开关

```
<Quidway> debugging ppp all
```

2. 向日志主机（UNIX 工作站）输出日志信息配置举例

第一步：路由器侧配置如下

(1) 开启信息中心。

```
[Quidway] info-center enable
```

(2) 将 IP 地址为 202.38.1.10 的 UNIX 工作站用作日志主机，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 PPP 和 IP，使用 UNIX 设备 Local4。

```
[Quidway] info-center loghost 202.38.1.10 language english
[Quidway] info-center loghost 202.38.1.10 facility local4
[Quidway] info-center source ppp channel loghost log level informational
[Quidway] info-center source ip channel loghost log level informational
```

第二步：日志主机侧配置如下

UNIX 主机上也要进行相应设置以完成上述功能。下面以 SunOS 4.0 举例说明，其它厂商 UNIX 操作系统上的配置操作基本与之相同。

(3) 以超级用户（root）的身份执行以下命令

```
# mkdir           /var/log/Quidway
# touch           /var/log/Quidway/information
```

(4) 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：

- 注释只允许独立成行，并以字符#开头。
- 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。
- 在文件名之后不得有多余的空格。

/etc/syslog.conf 中指定的设备名及接受的日志信息级别与路由器上配置的 **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。

当日志文件 config 建立且/etc/syslog.conf 文件被修改了之后，应执行以下命令，给系统守护进程 syslogd 发一个 HUP 信号，使 syslogd 重新读取它的配置文件/etc/syslog.conf。

```
#ps -ae | grep syslogd
147
#kill -HUP 147
```

进行以上操作后，路由器的相关信息就可以输出到相应的日志文件中了。

上面的配置只向日志主机输出严重程度为 informatinal 及以上的日志信息，即级别为 0～6 的日志信息。

日志信息的最低级别为 debugging，设置为 debugging 将导致所有的日志信息都发送到日志主机，对系统性能可能产生影响，因此，通常情况下，不建议用户将日志信息级别设置为 debugging

📖 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。

2.4 设备运行显示和调试－AR 46 系列

设备运行管理负责完成监控设备的运行状态和配置设备的各项参数等功能。从功能类型上看，设备运行管理包括显示、复位、设置等。以下几个方面：

1. 设备显示命令

请在任何视图下进行下列操作。

表2-23 设备信息显示命令

操作	命令
显示设备基本信息	**display device** *slot-number*
显示环境信息	**display environment**
设备告警信息和状态信息的显示	**display alarm urgent** [**time | slot | id**]
查看路由器 **schedule reboot** 终端服务相关参数设置情况。	**display schedule reboot**

2. 设备复位命令

请在用户视图下进行下列配置。

表2-24 设备复位命令

操作	命令
清除所有当前储存的告警信息	**reset alarm urgent**

3. 设备配置命令

请在系统视图下进行下列配置。

表2-25 设备配置命令

操作	命令
文件的在线升级	**upgrade** [**bootrom | pico-code | logic**] *filename*
启动路由器的定时重启功能，并设置具体的重启日期和时间。	**schedule reboot at** *time* [*date*]
使能路由器定时重启功能，并设定等待时延。	**schedule reboot delay** { *time* | *minutes* }
取消 **schedule reboot** 终端服务的参数设置。	**undo schedule reboot**

4. 配置热插拔预处理

请在用户视图下进行下列配置。

表2-26 配置热插拔预处理

操作	命令
配置热插拔预处理命令	**remove slot** *slotnum*
取消热插拔预处理	**undo remove slot** *slotnum*

在热插拔接口卡之前必须执行命令 **remove slot** 做预处理。如果错误地执行了该命令而不想拔出接口卡，则可以通过执行 **undo remove slot** 来取消刚才的操作。接口板被拔出并重新插入时不必执行 **undo remove slot** 命令。

第3章 HWPing 配置

3.1 HWPing 简介

HWPing 是测量网络上运行的各种协议性能的一种工具，它是对 ping 功能的增强。ping 功能只能使用 ICMP 协议来测试数据包在本端和指定的目的端之间的往返时间；然而 HWPing 不但可以完成上面的功能，还可以探测 DLSw、dhcp、FTP、HTTP、SNMP 服务器是否打开以及测试各种服务的响应时间等。

可以通过网管来设置 HWPing 操作的各项参数，并启动 HWPing，最后查看操作的结果，也可以通过 display hwping result 命令来查看 HWPing 操作的统计结果。

图3-1 HWPing 客户端和服务器之间的关系图

3.2 HWPing 的配置

用户在使用 HWPing 功能之前首先必须分别配置好 HWPing 服务器和 HWPing 客户端。

3.2.1 HWPing 服务器的配置

HWPing 服务器的配置包括：

- 使能服务器
- 配置 HWPing 服务器监听的服务

1. 使能服务器

HWPing 功能中有些测试操作，如 jitter（对 UDP 报文传输的延时变化分析）、指定端口的 UDP 测试和指定端口的 TCP 测试等，需要服务器和客户端配合才能完成，HWPing 服务器负责处理 HWPing 客户端发来的测试包。只有在路由器上使能了 HWPing 服务器功能，HWPing 服务器才能工作。

可以在同一台路有器上同时使能 HWPing 客户端和 HWPing 服务器。也就是说，同一台路由器既可以做 HWPing 服务器，又可以做 HWPing 客户端。

请在系统视图下进行下列配置。

表3-1 使能服务器

操作	命令
使能服务器功能	**hwping-server enable**
关闭服务器功能	**undo hwping-server enable**

缺省情况下，关闭服务器功能。

2. 配置 udp 监听服务

对于 TCP 和 UDP 的 HWPing 测试，HWPing 服务器通过监听功能响应客户端发起的测试。HWPing 服务器只对特定的客户端进行响应，即只有在 HWPing 服务器上配置了相应的目的地址和端口号的客户端才能得到服务器的响应。

可以在一个 HWPing 服务器上创建多个 TCP 和 UDP 监听服务，每个监听服务对应一个指定的目的地址和端口号。

请在系统视图下进行下列配置。

表3-2 配置 udp 监听端口

操作	命令
配置 UDP 监听服务	**hwping-server udpecho** *ip-address port-num*
取消 UDP 监听服务	**undo hwping-server udpecho** *ip-address port-num*
配置 TCP 监听服务	**hwping-server tcpconnect** *ip-address port-num*
取消 TCP 监听服务	**undo hwping-server tcpconnect** *ip-address port-num*

缺省情况下，未配置 UDP 和 TCP 监听服务。

3.2.2 HWPing 客户端的配置

HWPing 客户端的配置包括：

- 使能客户端
- 建立测试组
- 配置同时能进行测试的最大数目
- 配置 trap 开关

1. 使能客户端

只有使能了 HWPing 客户端功能，才能进行各类测试的设置和测试。

请在系统视图下进行下列配置。

表3-3 使能客户端

操作	命令
打开客户端	**hwping-agent enable**
关闭客户端	**undo hwping-agent enable**

缺省情况下，关闭 HWPing 客户端。

2. 建立测试组

HWPing 测试组是一个 HWPing 测试项的集合。一个测试组中可以包含若干个测试项目。每个测试组都有一个管理员名称和一个操作标签。管理员名称和操作标签可以唯一确定一个测试组。

建立了测试组并配置好测试项参数之后就可以在测试组中通过测试命令进行 HWPing 测试。

在系统视图下进行下列配置。

表3-4 建立测试组

操作	命令
建立测试组	**hwping** *administrator-name operation- tag*
删除测试组	**undo hwping** *administrator-name operation-tag*

缺省情况下，没有配置测试组。

HWPing 测试组包含以下参数：

- 目的地址
- 目的端口
- 源接口
- 源地址
- 源端口
- 测试类型
- 一次测试发送报文的个数
- ICMP 数据包的大小
- 发送报文的时间间隔
- 测试超时时间
- 报文生存时间
- 配置服务类型
- 报文填充字符

- HTTP 操作类型
- HTTP 操作字符串
- FTP 操作类型
- FTP 操作用户名
- FTP 操作密码
- FTP 操作文件名
- 保存历史记录的最大数目
- 测试描述

(1) 配置目的地址

目的地址指的是 HWPing 服务器的 IP 地址，相当于 ping 命令中的目的地址。该目的地址必须是 HWPing 服务器上配置了 TCP 或 UDP 监听服务的 IP 地址。

请在 HWPing 测试组视图下进行下列配置。

表3-5 配置目的地址

操作	命令
配置 HWPing 服务器目的地址	**destination-ip** *ipaddress*
删除 HWPing 服务器目的地址	**undo destination-ip**

缺省情况下，没有配置 HWPing 服务器目的地址。

(2) 配置目的端口

在进行 TCP 或 UDP 测试时必须指定 HWPing 服务器的端口号。该端口号必须是 HWPing 服务器上配置了 TCP 或 UDP 监听服务的端口号。

请在 HWPing 测试组视图下进行下列配置。

表3-6 配置目的端口

操作	命令
配置 HWPing 服务器目的端口	**destination-port** *port-number*
删除 HWPing 服务器目的端口	**undo destination-port**

缺省情况下，没有配置 HWPing 服务器目的端口。

(3) 配置源接口

在进行 DHCP 测试时，可以指定发送 DHCP 请求报文使用的源接口。如果指定了源接口，那么在测试 DHCP 时，系统将直接使用该源接口发送 DHCP 请求报文，而不是通过路由来确定发送报文的接口。另外，DHCP 请求报文中的源 IP 地址将使用该接口的 IP 地址。

请在 HWPing 测试组视图下进行下列配置。

表3-7 绑定源接口

操作	命令
绑定源接口	**source-interface** *interface-type interface-number*
删除源接口	**undo source-interface**

缺省情况下，没有配置源接口。

(4) 配置源地址

在进行 DHCP 测试时，可以指定发送 DHCP 请求报文指中的源 IP 地址，这样 DHCP 服务器将使用此 IP 地址作为 DHCP 响应报文的目的地址。

请在 HWPing 测试组视图下进行下列配置。

表3-8 配置源地址

操作	命令
配置源地址	**source-ip** *ipaddress*
删除源地址	**undo source-ip**

缺省情况下，没有指定源 IP 地址。

(5) 配置源端口

在进行 DHCP 测试时，可以指定发送 DHCP 请求报文的源端口号，这样 DHCP 服务器将使用此端口号作为 DHCP 响应报文的目的端口号。

请在 HWPing 测试组视图下进行下列配置。

表3-9 配置源端口

操作	命令
配置源端口	**source-port** *port-number*
删除源端口	**undo source-port**

缺省情况下，没有指定源端口。

(6) 配置测试类型

HWPing 可以测试很多种类型的连接。但是每一次测试只能测试某一种类型，也就是说每一个测试组只能是某一类型的 HWPing 测试。

HWPing 的测试类型包括：**icmp、udppublic、udpprivate、tcppublic、tcpprivate、dlsw、dhcp、snmpquery、ftp、http。**

请在 HWPing 测试组视图下进行下列配置。

表3-10 配置测试类型

操作	命令
配置测试类型	**test-type** { **icmp** | **udppublic** | **udpprivate** | **tcppublic** | **tcpprivate** | **dlsw** | **dhcp** | **snmpquery** | **ftp** | **http** }

缺省情况下，测试类型为 ICMP。

(7) 配置发送测试报文的个数

如果配置一次测试发送报文的个数大于 1，那么系统在发送第一个测试报文之后，如果收到响应报文就发送第二个测试报文。如果一直没有收到响应报文，则等到测试定时器超时，发送第二个测试报文。如此直到发送完最后一个测试报文。该参数相当于 ping 命令中的“ -**n** ”参数。

请在 HWPing 测试组视图下进行下列配置。

表3-11 配置发送测试报文的个数

操作	命令
配置发送测试报文的个数	**count** *times*
恢复发送测试报文的个数到默认值	**undo count** *times*

缺省情况下，一次测试报文的个数为 1。

(8) 配置 ICMP 数据包的大小

ICMP 数据包的大小是指进行 ICMP 测试时 ECHO-REQUEST 报文长度（不包括 IP 和 ICMP 报文头）。该参数相当于 ping 命令中的“ -**s** ”参数。

请在 HWPing 测试组视图下进行下列配置。

表3-12 配置数据包的大小

操作	命令
配置数据包的大小	**datasize** *size*
恢复为默认值	**undo datasize**

缺省情况下，数据包的大小为 60。

(9) 配置自动测试的时间间隔

配置自动测试使系统自动的每隔一段时间就进行一次测试。

请在 HWPing 测试组视图下进行下列配置。

表3-13 配置自动测试的时间间隔

操作	命令
配置自动测试的时间间隔	**frequency** *interval*
取消自动测试	**undo frequency**

缺省情况下，自动测试的时间间隔为 0，即只进行一次测试。

(10) 配置置测试超时时间

测试超时时间是指发送完 ECHO-REQUEST 后，等待 ECHO-RESPONSE 的时间，如果超过此时间还没有收到 ECHO-RESPONSE，则认为该次测试不通。该参数相当于 ping 命令中的“ **-t** ”参数，但是时间单位不一样。

请在 HWPing 测试组视图下进行下列配置。

表3-14 配置测试超时时间

操作	命令
配置测试超时时间	**timeout** *time*
恢复为默认值	**undo timeout**

缺省情况下，超时时间为 3 秒。

(11) 配置报文生存时间

报文生存时间是指测试报文的 ttl 值。该参数相当于 ping 命令中的“ **-i** ”参数。

请在 HWPing 测试组视图下进行下列配置。

表3-15 配置报文生存时间

操作	命令
配置 ttl	**ttl** *number*
取消配置	**undo ttl**

缺省情况下，根据路由器的发送属性决定。

(12) 配置服务类型

服务类型是指 IP 报文头中的 ToS 域值。该参数相当于 ping 命令中的“ **-o** ”参数

请在 HWPing 测试组视图下进行下列配置。

表3-16 配置服务类型

操作	命令
配置服务类型	**tos** *value*
恢复默认值	**undo tos**

缺省情况下，服务类型为 0。

(13) 报文填充字符

进行 ICMP 测试时，要对所发送的 ICMP 报文的数据段的内容进行填充。填充时，如果测试数据包大小比配置的填充数据小，那么只使用此字符串的前一部分；如果测试数据包大小比配置的填充数据大，那么将使用此字符串循环进行填充。例如，配置填充数据为“ abcd ”，当测试数据包大小为 3 时，则只使用“ abc ”作为填充数据；当测试数据包大小为 6 时，则只使用“ abcdab ”作为填充数据。

请在 HWPing 测试组视图下进行下列配置。

表3-17 配置报文填充字符

操作	命令
配置填充字符	**datafill** *string*
取消填充字符	**undo datafill**

缺省情况下，从 0 到 255 循环填充数据。

(14) 配置 HTTP 操作类型

HWPing 客户端可以配置和服务器端进行 HTTP 交互的类型。

此配置必须在测试类型为 HTTP 时进行。

请在 HWPing 测试组视图下进行下列配置。

表3-18 配置 HTTP 操作类型

操作	命令
配置操作类型	**http-operation** { **get** | **post** }

缺省情况下，使用 get 操作。

(15) 配置 HTTP 的 URL

配置和 HTTP 服务器交换所使用的 URL，该 URL 指定所访问的页面，以及所使用的 HTTP 的版本。

此配置必须在测试类型为 HTTP 时进行。

请在 HWPing 测试组视图下进行下列配置。

表3-19 配置 HTTP 的 URL

操作	命令
配置 HTTP 的 URL	**http-string** *url-string*
删除 HTTP 的 URL	**undo http-string**

缺省情况下，没有配置 HTTP 的 URL。

(16) 配置 FTP 操作类型

HWPing 客户端可以配置和服务器端进行 FTP 交互的类型。

此配置必须在测试类型为 FTP 时进行。

请在 HWPing 测试组视图下进行下列配置。

表3-20 配置 FTP 操作类型

操作	命令
配置操作类型	**ftp-operation** { **get** | **put** }

缺省情况下，FTP 操作类型为 get 操作。

(17) 配置 FTP 操作用户名和密码

进行 FTP 操作时需要使用用户名和密码。

此配置必须在测试类型为 FTP 时进行。

请在 HWPing 测试组视图下进行下列配置。

表3-21 配置 FTP 操作用户名和密码

操作	命令
配置用户名	**username** *name*
删除用户名	**undo username**
配置密码	**password** *password*
删除密码	**undo password**

缺省情况下，没有配置用户名和密码。

(18) 配置 FTP 操作文件名

配置 FTP 所要操作的服务器端的文件名。

此配置必须在测试类型为 FTP 时进行。

请在 HWPing 测试组视图下进行下列配置。

表3-22 配置 FTP 操作文件名

操作	命令
配置文件名	**filename** *file-name*
删除文件名	**undo filename**

缺省情况下，没有配置操作的文件名。

(19) 配置 Jitter 测试时发送的测试包个数

Jitter 测试是为了对 UDP 报文传输的延时变化进行统计分析，在测试时，源端会以一定的时间间隔（可配置）发送一系列的数据包，目的端收到数据包后，将数据包打上时间戳，然后再发回到源端。源端收到数据包后就可计算出抖动时间。因此每次探测必须发送多个测试包进行测试。每次探测发送的测试包个数越多，统计分析越准确，但完成测试所需的时间也越长。

此配置必须在测试类型为 Jitter 时进行。

请在 HWPing 测试组视图下进行下列配置。

表3-23 配置 Jitter 测试时发送的测试包个数

操作	命令
Jitter 测试时发送的测试包个数	**jitter-packetnum** *number*
恢复为默认值	**undo jitter-packetnum**

缺省情况下，Jitter 测试时发送的测试包为 20 个。

(20) 配置 Jitter 测试时发送测试包的时间间隔

Jitter 测试每次探测都要发送多个 UDP 测试包，可以配置发送测试包的时间间隔。发送测试包的时间间隔越小，完成测试就越快，但是发送测试包的时间间隔太小可能会对网络带来一定的冲击。

此配置必须在测试类型为 Jitter 时进行。

请在 HWPing 测试组视图下进行下列配置。

表3-24 配置 Jitter 测试时发送测试包的时间间隔

操作	命令
Jitter 测试时发送测试包的时间间隔	**jitter-interval** *interval*
恢复为默认值	**undo jitter-interval**

缺省情况下，Jitter 测试时发送测试包的时间间隔为 20 毫秒。

(21) 配置保存历史记录的最大数目

指定在一个测试组中能保存的历史记录数的最大数目，当超过这个数目时，它会丢弃最先测试的结果。

请在 HWPing 测试组视图下进行下列配置。

表3-25 配置保存历史记录的最大数目

操作	命令
配置保存历史记录的最大数目	**history-records** *number*
恢复为默认值	**undo history-records**

缺省情况下，最大历史记录数为 50 条。

(22) 配置路由表旁路

路由表旁路是指，远端主机将不进行通常的路由表查找，而直接发送 ICMP 报文到相连网络上的主机。如果主机所在网络不是直连的，就返回错误。例如，在接口上 ping 一个无路由的本地主机时可以使用本功能。

请在 HWPing 测试组视图下进行下列配置。

表3-26 配置路由表旁路

操作	命令
启动路由表旁路功能	**sendpacket passroute**
关闭路由表旁路功能	**undo sendpacket passroute**

缺省情况下，关闭路由表旁路功能。

(23) 配置 VPN instance 信息

请在 HWPing 测试组视图下进行下列配置。

表3-27 配置 VPN instance 信息

操作	命令
设置 ICMP 的 VPN instance 信息	**vpninstance** *name*
取消 ICMP 的 VPN instance 信息	**undo vpninstance**

缺省情况下，未设置 ICMP 的 VPN instance 信息。

(24) 配置测试组描述

用户可以对一个测试组进行简要的描述。通常用于描述一个测试组所做的测试项或测试的目的。

请在 HWPing 测试组视图下进行下列配置。

表3-28 配置测试描述

操作	命令
配置测试描述	**description** *string*
取消测试描述	**undo description**

缺省情况下，无任何描述信息。

(25) 配置 trap

HWPing 测试成功或者失败都会产生 trap 信息，可以通过设置 trap 开关控制是否向网管发送该 trap。

可以设置 HWPing 测试以及每一次测试内的探测连续失败若干次才发送 trap。缺省情况下，探测一次失败及测试一次失败就发送 trap。

请在 HWPing 测试组视图下进行下列配置。

表3-29 打开 trap 开关

操作	命令
打开 trap 开关	**send-trap** { **all**| **probefailure**	**testcomplete**	**testfailure** }
关闭 trap 开关	**undo send-trap** { **all**| **probefailure**	**testcomplete**	**testfailure** }
设置 HWPing 测试连续多少次测试失败之后发送 Trap	**test-failtimes** *times*
设置 HWPing 测试连续多少次探测失败之后发送 Trap	**probe-failtimes** *times*

缺省情况下，不发送 trap 到网管站。

3. 配置同时能进行测试的最大数目

可以设定一个路由器（HWPing 客户端）最多能同时进行测试的数目。如果设定为 0，表示没有限制。

请在系统视图下进行下列配置。

表3-30 配置同时进行测试的最大数目

操作	命令
设定最大数目	**hwping-agent max-requests** *number*
恢复最大数目的缺省值	**undo hwping-agent max-requests** *number*

缺省情况下，最大数目为 5 条。

3.3 执行测试

建立了测试组并配置好测试项参数之后就可以在测试组中通过测试命令进行 HWPing 测试。

请在 HWPing 测试组视图下进行下列配置。

表3-31 测试

操作	命令
执行测试	**test-enable**

📖 说明：

HWPing 测试不会显示测试结果，要查看显示结果请使用显示测试信息命令。

3.4 显示测试结果信息

display hwping 命令可以分别用来查看测试的历史记录信息、jitter 信息和最新测试结果信息。

通过历史记录可以查看测试中记录的每一次探测的结果，历史记录的数目可以通过 **history-records** 命令进行设置。

通过最新测试结果可以查看最近一次测试的结果。

通过 jitter 信息可以查看 HWPing 进行 jitter 类型测试时记录的 UDP 报文传输的延时变化。其它类型的 HWPing 测试没有 jitter 信息。jitter 测试只记录最近的一次 jitter 信息。

请在所有视图下进行下列操作。

表3-32 显示测试信息

操作	命令
显示测试的结果信息	**display hwping** { **history** | **jitter** | **result** } [*administrator-name operation-tag*]

3.5 HWPing 典型配置举例

3.5.1 ICMP 测试

1. 介绍

HWPing ICMP 测试和 ping 测试一样，是使用 ICMP 协议来测试数据包在本端和指定的目的端之间的往返时间。

2. ICMP 测试配置步骤

📖 说明：

要想成功创建并启动一个 ICMP echo 功能的测试操作。必须执行以下步骤 1，2，3，6，其它步骤为可选项。

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 ICMP。

```
[router] hwping administrator icmp
```

步骤 2：配置测试的类型为 ICMP。

```
[router-hwping-administrator-icmp] test-type icmp
```

步骤 3：配置目的 IP 地址为 169.254.10.2。

```
[router-hwping-administrator-icmp] destination-ip 169.254.10.2
```

步骤 4：配置发送的测试包的个数。

```
[router-hwping-administrator-icmp] count 10
```

步骤 5：配置超时时间。

```
[router-hwping-administrator-icmp] timeout 3
```

步骤 6：启动测试操作。

```
[router-hwping-administrator-icmp] test-enable
```

步骤 7：查看测试结果。

```
[router-hwping-administrator-icmp] display hwping result administrator icmp
[router-hwping-administrator-icmp] display hwping history administrator icmp
```

3.5.2 DHCP 测试

1. 介绍

HWPing DHCP 测试用来测试从 DHCP 服务器分配到 IP 地址所需的时间。

2. DHCP 测试配置步骤

📖 说明：

要想成功创建并启动一个 DHCP 类型的测试。必须执行以下步骤 1，2，3，6，其它步骤为可选项。

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 DHCP。

```
[router] Hwping administrator dhcp
```

步骤 2：配置测试的类型为 DHCP。

```
[router-hwping-administrator-dhcp] test-type dhcp
```

步骤 3：配置源接口，此接口必须为以太口，DHCP 服务器位于和此接口相连的网络上。

```
[router-hwping-administrator-dhcp] source-interface ethernet1/0/0
```

步骤 4：配置测试的次数。

```
[router-hwping-administrator-dhcp] count 10
```

步骤 5：配置超时时间。

```
[router-hwping-administrator-dhcp] timeout 3
```

步骤 6：启动测试操作。

```
[router-hwping-administrator-dhcp] test-enable
```

步骤 7：查看测试结果。

```
[router-hwping-administrator-dhcp] display hwping result administrator dhcp
[router-hwping-administrator-dhcp] display hwping history administrator dhcp
```

3.5.3 DLSw 测试

1. 介绍

HWPing DLSw 测试用来测试 DLSw 设备的响应时间。

2. DLSw 测试配置步骤

📖 说明：

要想成功创建并启动一个 DLSw 类型的测试操作。必须执行以下步骤 1，2，3，6，其它步骤为可选项。而且在步骤 3 中所指定的目的路由器上必须使能 DLSw 功能（使用命令 **dlsw enable**），同时创建 DLSw 对（使用命令 **dlsw local** 和 **dlsw remote**），相关内容请参考本手册《VRP 操作手册》链路层协议的 DLSw 配置部分。

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 dlsw。

```
[router] Hwping administrator dlsw
```

步骤 2：配置测试的类型为 DLSw。

```
[router-hwping-administrator- dlsw] test-type dlsw
```

步骤 3：配置目的地址。

```
[router-hwping-administrator- dlsw] destination-ip 169.254.10.2
```

步骤 4：配置测试的次数。

```
[router-hwping-administrator- dlsw] count 10
```

步骤 5：配置超时时间。

```
[router-hwping-administrator- dlsw] timeout 3
```

步骤 6：启动测试操作。

```
[router-hwping-administrator- dlsw] test-enable
```

步骤 7：查看测试结果。

```
[router-hwping-administrator- dlsw] display hwping result administrator dlsw
[router-hwping-administrator- dlsw] display hwping history administrator dlsw
```

3.5.4 FTP 测试

1. 介绍

HWPing FTP 测试用来测试和指定的 FTP 服务器建立连接，及传送一个文件所用的时间。可以从 FTP 服务器得到一个文件，也可以向 FTP 服务器写一个文件。

2. FTP 测试配置步骤

📖 说明：

要想成功创建并启动一个 FTP 类型的测试操作。必须执行以下步骤 1，2，3，4，5，6，9 其它步骤为可选项。

配置以太网口 IP 地址。

```
[router] interface Ethernet 0/0/0
[router-Ethernet0/0/0 ] ip address 169.254.0.1 16
```

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 FTP。

```
[router] hwping administrator ftp
```

步骤 2：配置测试的类型为 FTP。

```
[router-hwping-administrator-ftp] test-type ftp
```

步骤 3：配置 FTP 服务器的 IP 地址为 169.254.10.2。

```
[router-hwping-administrator-ftp] destination-ip 169.254.10.2
```

步骤 4：配置用户名。

```
[router-hwping-administrator-ftp] username administrator
```

步骤 5：配置口令

```
[router-hwping-administrator-ftp] password hwping
```

步骤 6：配置要获取的文件名。

```
[router-hwping-administrator-ftp] filename config.txt
```

步骤 7：配置测试的次数。

```
[router-hwping-administrator-ftp] count 10
```

步骤 8：配置超时时间。

```
[router-hwping-administrator-ftp] timeout 30
```

步骤 9：配置源地址。

```
[router-hwping-administrator-ftp] source-ip 169.354.0.1
```

步骤 10：启动测试操作。

```
[router-hwping-administrator-ftp] test-enable
```

步骤 11：查看测试结果。

```
[router-hwping-administrator-ftp] display hwping result administrator ftp
```

```
[router-hwping-administrator-ftp] display hwping history administrator ftp
```

对端仅需要启动 FTP Server，并配置相应的用户即可。

3.5.5 HTTP 测试

1. 介绍

HWPing HTTP 测试用来测试与指定的 HTTP 服务器之间建立连接并从 HTTP 服务器获取一个文件所用的时间。

2. HTTP 测试配置步骤

📖 说明：

要想成功创建并启动一个 HTTP 类型的测试操作。必须执行以下步骤 1，2，3，4，其它步骤为可选项。

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 HTTP。

```
[router] Hwping administrator http
```

步骤 2：配置测试的类型为 HTTP。

```
[router-hwping-administrator-http] test-type http
```

步骤 3：配置 HTTP 服务器的 IP 地址为 169.254.10.2。

```
[router-hwping-administrator-http] destination-ip 169.254.10.2
```

步骤 4：配置 URL。

```
[router-hwping-administrator-http] http-string
```

步骤 5：配置测试的次数。

```
[router-hwping-administrator-http] count 10
```

步骤 6：配置超时时间。

```
[router-hwping-administrator-http] timeout 30
```

步骤 7：启动测试操作。

```
[router-hwping-administrator-http] test-enable
```

步骤 8：查看测试结果。

```
[router-hwping-administrator-http] display hwping result administrator http
[router-hwping-administrator-http] display hwping history administrator http
```

3.5.6 Jitter 测试

1. 介绍

HWPing Jitter 测试用来测试本端(HWPing 客户端)和指定的目的端（HWPing 服务器）之间传送 UDP 报文的抖动时间。

2. Jitter 测试配置步骤

📖 说明：

要想成功创建并启动一个 Jitter 类型的测试操作。必须在 HWPing 客户端执行以下步骤 1，2，3，4，8 其它步骤为可选项。

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 Jitter。

```
[router] Hwping administrator jitter
```

步骤 2：配置测试的类型为 Jitter。

```
[router-hwping-administrator-jitter] test-type jitter
```

步骤 3：配置 HWPing 服务器的 IP 地址为 169.254.10.2。

```
[router-hwping-administrator-jitter] destination-ip 169.254.10.2
```

步骤 4：配置 HWPing 服务器的目的端口。

```
[router-hwping-administrator-jitter] destination-port 9000
```

步骤 5：配置测试的次数。

```
[router-hwping-administrator-jitter] count 10
```

步骤 6：配置超时时间。

```
[router-hwping-administrator-jitter] timeout 30
```

步骤 7：启动测试操作。

```
[router-hwping-administrator-jitter] test-enable
```

步骤 8：查看测试结果。

```
[router-hwping-administrator-jitter] display hwping result administrator jitter
[router-hwping-administrator-jitter] display hwping history administrator jitter
[router-hwping-administrator-jitter] display hwping jitter administrator jitter
```

⚠ 注意：

必须在目的端启动 HWPing 服务器，目的端的配置如下：

[router]**hwping-server enable**

[router]**hwping-server udpecho 169.254.10.2 9000**

在 HWPing 服务器上使用命令 **hwping-server udpecho** 创建响应 UDP 包的 HWPing 服务器时，指定的 IP 地址和端口号是服务器所要处理的包的目的地址和目的端口。它们必须和上面步骤 3，4 中配置的 IP 地址和端口号一样。

3.5.7 SNMP 测试

1. 介绍

HWPing SNMP 测试用来测试从发出一个 snmp 协议查询包到接收到响应所用的时间。

2. SNMP 测试配置步骤

📖 说明：

要想成功创建并启动一个 SNMP 类型的测试操作，必须在 HWPing 客户端执行以下步骤 1，2，3，6，其它步骤为可选项。

使能 SNMP 客户端。

```
[router ] snmp-agent trap enable
```

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 snmp。

```
[router] Hwping administrator snmp
```

步骤 2：配置测试的类型为 SNMP。

```
[router-hwping-administrator-snmp] test-type snmpquery
```

步骤 3：配置 目的 IP 地址为 169.254.10.2。

```
[router-hwping-administrator-snmp] destination-ip 169.254.10.2
```

步骤 4：配置测试的次数。

```
[router-hwping-administrator-snmp] count 10
```

步骤 5：配置超时时间。

```
[router-hwping-administrator-snmp] timeout 30
```

步骤 6：启动测试操作。

```
[router-hwping-administrator-snmp] test-enable
```

步骤 7：查看测试结果。

```
[router] display hwping result administrator snmp
[router] display hwping history administrator snmp
```

⚠ 注意：

在上面步骤 3 中配置的目的 IP 地址所指定的机器上必须启动网管功能，否则将收不到回应包。在本公司路由器上可使用 **snmp-agent** 命令启动网管功能，相关内容请参考本手册 SNMP 配置部分。

3.5.8 指定端口的 TCP 测试

1. 介绍

指定端口的 HWPing TCP 测试用来测试本端和指定的目的端之间建立 TCP 连接的时间。

2. 指定端口的 TCP 测试配置步骤

📖 说明：

要想成功创建并启动一个 TCP 类型的测试操作。必须执行以下步骤 1，2，3，4，7，其它步骤为可选项。

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 tcpprivate。

```
[router] Hwping administrator tcpprivate
```

步骤 2：配置测试的类型为 tcpprivate。

```
[router-hwping-administrator- tcpprivate] test-type tcpprivate
```

步骤 3：配置 HWPing 服务器的 IP 地址为 169.254.10.2。

```
[router-hwping-administrator- tcpprivate] destination-ip 169.254.10.2
```

步骤 4：配置 HWPing 服务器的目的端口。

```
[router-hwping-administrator- tcpprivate] destination-port 9000
```

步骤 5：配置发送的测试包的个数。

```
[router-hwping-administrator- tcpprivate] count 10
```

步骤 6：配置超时时间。

```
[router-hwping-administrator- tcpprivate] timeout 3
```

步骤 7：启动测试操作。

```
[router-hwping-administrator- tcpprivate] test-enable
```

步骤 8：查看测试结果。

```
[router] display hwping result administrator tcpprivate
[router] display hwping history administrator tcpprivate
```

⚠ 注意：

必须在目的端启动 HWPing 服务器并创建 HWPing TCP 监听服务，在目的端的配置如下：

[router]**hwping-server enable**

[router]**hwping-server tcpconnect 169.254.10.2 9000**

在 HWPing 服务器上使用命令 **hwping-server tcpconnect** 创建建立 TCP 监听服务时，指定的 IP 地址和端口号必须和上面步骤 3，4 中配置的 IP 地址和端口号一样。

3.5.9 指定端口的 UDP 测试

1. 介绍

指定端口的 HWPing UDP 测试用来测试本端和指定的目的端之间 UDP 协议包的往返时间。

2. 指定端口的 UDP 测试配置步骤

📖 说明：

要想成功创建并启动一个指定端口的 UDP 类型的测试操作。必须执行以下步骤 1，2，3，4，7，其它步骤为可选项。

使能 hwping 客户端。

```
[router ] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 udpprivate。

```
[router] Hwping administrator udpprivate
```

步骤 2：配置测试的类型为 udpprivate。

```
[router-hwping-administrator-udpprivate] test-type udpprivate
```

步骤 3：配置 HWPing 服务器的 IP 地址为 169.254.10.2。

```
[router-hwping-administrator-udpprivate] destination-ip 169.254.10.2
```

步骤 4：配置 HWPing 服务器的目的端口。

```
[router-hwping-administrator-udpprivate] destination-port 9000
```

步骤 5：配置发送的测试包的个数。

```
[router-hwping-administrator-udpprivate] count 10
```

步骤 6：配置超时时间。

```
[router-hwping-administrator-udpprivate] timeout 3
```

步骤 7：启动测试操作。

```
[router-hwping-administrator-udpprivate] test-enable
```

步骤 8：查看测试结果。

```
[router] display hwping result administrator udpprivate
[router] display hwping history administrator udpprivate
```

⚠ 注意：

要在目的端启动 HWPing 服务器，需进行如下配置：

[router]**hwping-server enable**

[router]**hwping-server udpecho 169.254.10.2 9000**

在 HWPing 服务器上使用命令 **hwping-server udpecho** 创建响应 UDP 包的 HWPing 服务时，指定的 IP 地址和端口号是服务器所要处理的包的目的地址和目的端口。它们必须和上面步骤 3，4 中配置的 IP 地址和端口号一样。

第4章 文件管理

4.1 文件系统

4.1.1 文件系统简介

文件系统的主要功能为管理存储设备，把文件保存在存储设备中。路由器目前支持的存储设备是 FLASH。

文件系统是指对存储设备中的文件、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。这些操作，请在用户视图下执行。请注意文件全名最多支持 64 字节，超长文件名将导致您不能正常进行操作。

4.1.2 目录操作

文件系统可以创建并删除目录，以及显示当前的工作目录，显示指定目录下的文件或目录信息。

请在用户视图下进行下列操作。

表4-1 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** | /**h**] [*file-url*]
改变当前目录	**cd** *directory*

4.1.3 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、执行批处理文件、显示指定文件的信息和私有文件信息，如下表所示。

1. 一般操作

请在用户视图下进行下列操作，其中 **execute** 命令在系统视图下执行。

表4-2 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** [*filename*] [flash:/] [**/force**]
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** | /*h*] [*file-url*]
执行批处理文件	**execute** *filename*

2. 配置 dual image 功能

在 Flash 大于 8M 的路由器上可以加载提供 dual image 功能的软件版本，此时系统缺省定义了三个用于启动的应用程序文件：主程序文件、备份程序文件、安全程序文件。当用户在 Flash 中加载了这三个应用程序文件时，系统将依次选择使用这三个文件来启动路由器。主程序文件、备份程序文件、安全程序文件的缺省文件名、类型及启动时的选择顺序如下：

- 主文件，缺省文件名为 main.bin，文件类型为 M，是系统启动缺省使用的文件；
- 备份文件，缺省文件名为 backup.bin，文件类型为 B。当主文件启动失败时，系统使用备份文件启动；
- 安全文件，缺省文件名为 secure.bin，文件类型为 S。当备份文件启动失败时，系统使用安全文件启动；如安全文件启动失败，系统将提示启动失败信息。

用户可以使用下面命令显示 Flash 中的文件，选择主文件/备份文件。

请在系统视图下配置如下命令：

表4-3 配置 dual image 功能

操作	命令
显示 Flash 中所有启动文件。	**bootfile dir**
指定路由器启动时使用的主程序文件。	bootfile main { *main-bootfile-name* }
指定路由器启动时使用的备份程序文件。	**bootfile backup** { *backup-bootfile-name* }

📖 说明：

由于安全文件为保证系统正常启动的最后一项保证措施，故安全文件的文件类型不允许修改，安全文件也不能由其它类型的文件修改而来，只能由用户在 Boot ROM 菜单中下载，而且安全文件名必须指定为 secure.bin。如果用户在系统启动后使用 **rename** 命令改变了安全文件名，那么 Flash 中就没有了安全文件，需要用户重新下载。

用户还可以在 Boot ROM 菜单中进行以上操作，具体方法请参见相关设备的安装手册。

4.1.4 存储设备操作

文件系统可以格式化指定的存储设备，请在用户视图下进行下列操作。

表4-4 存储设备操作

操作	命令
格式化存储设备	**format** *device-name*

4.1.5 文件系统提示方式

用户通过命令可以修改当前文件系统的提示方式。

请在系统视图下进行下列操作。

表4-5 设置文件系统提示方式

操作	命令
文件系统的提示方式	**file prompt** { **alert** | **quiet** }

4.1.6 文件系统使用举例

查看根目录及 test 目录下当前的文件。

```
<Quidway> dir
Directory of *
   0   -rw-   2145123  Jul 12 2001 12:28:08   AR46.bin
   1   -rw-       595   Jul 12 2001 10:47:50   vrpcfg.txt
   2   drw-         0  Jul 12 2001 19:41:20   test
6477 KBytes total (2144 KBytes free)
<Quidway> dir flash:/test/
Directory of flash:/test/
   0   drw-         -  Jul 12 2001 20:23:37   subdir
```

```
   1   -rw-       595  Jul 12 2001 20:13:19   vrpcfg.txt
   2   -rw-        50  Jul 12 2001 20:08:32   sample.txt
6477 KBytes total (2144 KBytes free)
```

移动文件从 flash:/test/sample.txt 到 flash:/sample.txt。

```
<Quidway> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]:y
% Moveded file flash:/test/sample.txt flash:/sample.txt
```

查看移动后的显示结果。

```
<Quidway> dir
Directory of *
   0   -rw-   2145123  Jul 12 2001 12:28:08   ne80.bin
   1   -rw-       595   Jul 12 2001 10:47:50   vrpcfg.txt
   2   drw-         0   Jul 12 2001 19:41:20   test
   3   -rw-        50   Jul 12 2001 20:26:48   sample.txt
6477 KBytes total (2144 KBytes free)
<Quidway> dir flash:/test/
Directory of flash:/test/
   0   drw-             Jul 12 2001 20:23:37   subdir
   1   -rw-       595   Jul 12 2001 20:13:19   vrpcfg.txt
6477 KBytes total (2144 KBytes free)
```

4.2 FTP 配置

4.2.1 FTP 简介

FTP 协议在 TCP/IP 协议族中属于应用层协议，主要向用户提供与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。

系统提供的 FTP 服务包括：

- FTP Server 服务，用户可以运行 FTP 客户端程序登录到路由器上，访问路由器上的文件。
- FTP Client 服务，用户通过终端仿真程序或 Telnet 程序建立与路由器的连接后，可以通过输入 FTP 命令，建立路由器与远程 FTP Server 的连接，并访问远程主机上的文件。

FTP 服务器配置包括：

- 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 服务器的显示和调试

4.2.2 启动 FTP 服务器

只有启动 FTP 服务器功能，FTP 客户端才能登录到服务器上，访问服务器上的文件。

请在系统视图下进行下列配置。

表4-6 启动 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 服务器支持多个用户的同时访问。远端 FTP 用户客户端向 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。

4.2.3 配置 FTP 服务器的验证和授权

FTP 服务器的授权配置信息包含提供给 FTP 用户的工作目录的路径的配置等。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。在使用 FTP 服务时，必须事先在路由器上配置好用户类型和 FTP 工作目录。

表4-7 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，并且进入本地用户视图（系统视图）	**local-user** *user-name*
删除指定的本地用户	**undo local-user** { *user-name* **| all** }
配置 FTP 用户的密码（本地用户视图）	**password [cipher | simple]** *password*
取消 FTP 用户的密码（本地用户视图）	**undo password**
配置 FTP 用户的授权信息（本地用户视图）	**service-type ftp [ftp-directory** *directory*]
恢复对 FTP 用户授权的缺省目录	**undo service-type ftp** [*ftp-directory*]

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 flash:/ftp/quidway（路由器文件系统支持的路径名）

配置 FTP 用户的验证及相关信息。

```
[Quidway] local-user quidway
[Quidway-luser-quidway] password simple huawei
[Quidway-luser-quidway] service-type ftp ftp-directory flash:/ftp/quidway
```

4.2.4 配置 FTP 服务器的运行参数

1. 设置 FTP 升级方式

用户从 PC 机登录到 FTP Server，使用 **put** 命令上载文件时，FTP Server 有两种升级方式，快速升级方式和普通升级方式。

- 快速升级方式，即 FTP Server 在全部接收完用户上载的文件后，再开始将该文件写入 Flash 中。采用这种方式，即使文件传送过程发生断电等异常情况，也不会损坏路由器的现有文件。
- 普通升级方式，即 FTP Server 一边接收用户的文件，一边将其写入 Flash 中。采用这种方式，可能会因为断电等异常情况导致路由器现有文件被损坏。与快速升级方式相比，普通升级方式只需要路由器较少的空闲内存。

请在系统视图下进行下列配置。

表4-8 设置 FTP 升级方式

操作	命令
设置 FTP 升级方式	**ftp update** { **fast** | **normal** }
恢复 FTP 缺省的升级方式	**undo ftp update** { **fast** | **normal** }

缺省情况下，FTP 服务器采用快速升级方式。

2. 设置 FTP 服务的连接时限

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。

请在系统视图下进行下列配置。

表4-9 配置 FTP 服务器的超时断连时间

操作	命令
配置 FTP 服务器的超时断开时间	**ftp timeout** *minutes*
恢复 FTP 服务器的超时断开时间的缺省值	**undo ftp timeout**

缺省情况下，连接空闲超时时间为 30 分钟。

4.2.5 FTP 服务器的显示和调试

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

表4-10 FTP 服务器的显示和调试命令

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

4.2.6 FTP 客户端介绍

FTP 客户端，作为路由器系统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。目前只支持一个 FTP 客户端。具体命令应用详见“ 命令手册 FTP 客户端命令 ”一节。

4.2.7 使用 FTP 升级 VRP 应用程序典型配置举例 1

1. 组网需求

使用 FTP 升级 VRP 主体软件，路由器作为 Client。FTP 服务器 IP 地址为 172.16.104.110。FTP 用户名为 8040，密码为 quidway。

2. 组网图

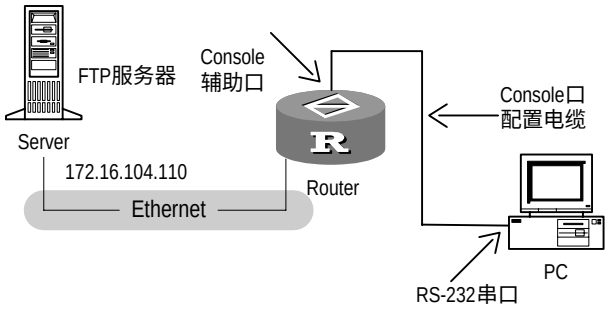

图4-1 利用 FTP Client 功能实现平滑升级

3. 配置步骤

请按如下方法进行操作：

#（提示）删除路由器存储设备中的多余文件，以保证剩余足够的空间，用于存储新的系统文件。

```
<Quidway> dir
Directory of flash:/

   0   -rw-   5709691  Jul 16 2004 16:17:30   secure.bin
```

```
  1   -rw-       939  Nov 29 2004 15:08:44   vrpcfg.cfg
  2   -rw-   8985472  Dec 19 2004 14:52:08   main.bin
  3   -rw-       969  Oct 29 2004 16:10:20   sip.cfg
  4   -rw-    524288  Nov 08 2004 14:32:41   bootromfull

31877 KB total (17007 KB free)
<Quidway> delete sip.cfg
```

以 FTP 方式登录服务器，获取系统主体软件，并存放于路由器存储设备的根目录下。

获取的系统文件必须存放在路由器存储设备的根目录下（flash:），文件名为“main.bin”。

```
<Quidway> ftp 172.16.104.110
Trying 172.16.104.110 ...
Connected to 172.16.104.110.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(172.16.104.110:(none)):8040
331 Give me your password, please
Password:xxxxxxx
230 Logged in successfully
[ftp] binary
[ftp] get vrp3.cc main.bin
200 PORT command okay
150 "D:\8040\system\vrp3.cc" file ready to send (5805100 bytes) in IMAGE / Binary mode
226 Transfer finished successfully.
FTP: 5805100 byte(s) received in 19.898 second(s) 291.74Kbyte(s)/sec.
[ftp] bye
```

升级成功后重新启动路由器，运行升级的版本。

4.2.8 使用 FTP 升级 VRP 应用程序典型配置举例 2

1. 组网需求

使用 FTP 升级 VRP 主体软件，路由器作为 Server。路由器以太网口的 IP 地址为 172.16.104.110。FTP 用户名为 8040，密码为 quidway。

2. 配置步骤

(1) 配置路由器

添加 FTP 授权用户名和密码。

```
[Quidway ] local-user 8040
[Quidway-luser-8040]password simple quidway
```

```
[Quidway-luser-8040]service-type ftp
[Quidway-luser-8040]ftp-directory flash:/ftp/quidway
```

启动 FTP 服务。

```
[Quidway ] ftp server enable
```

#（提示）删除路由器存储设备中的多余文件，以保证剩余足够的空间，用于存储新的系统文件。

```
<Quidway> dir
 Directory of flash:/

   0   -rw-   5709691  Jul 16 2004 16:17:30   secure.bin
   1   -rw-       939  Nov 29 2004 15:08:44   vrpcfg.cfg
   2   -rw-   8985472  Dec 19 2004 14:52:08   main.bin
   3   -rw-       969  Oct 29 2004 16:10:20   sip.cfg
   4   -rw-    524288  Nov 08 2004 14:32:41   bootromfull

31877 KB total (17007 KB free)
<Quidway> delete sip.cfg
```

(2) 配置 PC

以 FTP 方式登录路由器，上传 VRP 软件，并存放于路由器存储设备的根目录下。

```
ftp> put vrp3.cc main.bin
```

升级成功后重新启动路由器，运行升级的版本。

📖 说明：

利用 FTP 功能升级配置文件时，操作步骤与上述介绍完全一致，需要注意的是获取后的配置文件 vrpcfg.cfg 同样要放在路由器的根目录下（flash:）。

利用 FTP 远程升级 Boot ROM 程序时，请务必将文件名存为 bootromfull（烧片文件）或 bootrom（升级用文件），文件传送完成后再执行 **upgrade** 命令。

4.3 TFTP 配置

4.3.1 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 传输是由客户端发起的。当需要下载文件时，先由客户端向 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，

先由客户端向 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。路由器提供了 TFTP 客户端的功能。

4.3.2 TFTP 协议配置

1. 下载文件

请在用户视图下进行下列配置。

表4-11 用 TFTP 下载文件

操作	命令
用 TFTP 下载文件	**tftp** *X.X.X.X* **get** *source-filename* [*destination-filename*] [-**a** *ip-address*]
采用安全方式下载文件	**tftp** *X.X.X.X* **sget** *source-filename* [*destination-filename*] [-**a** *ip-address*]

⚠ 注意：

当采用安全方式下载时，要求当前系统内存有足够空间存放待下载文件。

2. 上传文件

请在用户视图下进行下列配置。

表4-12 用 TFTP 上传文件

操作	命令
用 TFTP 上传文件	**tftp** *X.X.X.X* **put** *source-filename* [*destination-filename*] [-**a** *ip-address*]

3. 设置相应的访问控制列表

该配置任务用来设置 TFTP 服务器访问控制列表，即与 **ACL** 命令设置的访问控制列表相关联，实现对远端 TFTP 服务器地址的访问控制。

请在系统视图下进行下列配置。

表4-13 设置访问控制列表

操作	命令
指定可以访问 TFTP 服务器的访问控制列表	**tftp-server acl** *acl-number*
删除设置的访问控制列表	**undo tftp-server acl**

4.4 XModem 配置

XModem 协议是一种文件传输协议，因其简单性和较好的性能而被广泛应用。XModem 协议是通过串口传输文件，支持 128 字节和 1K 字节两种类型的数据包，并且支持一般校验和、CRC 两种校验方式，在出现数据包错误的情况下支持多次重传（一般为 10 次）。

XModem 协议传输由接收程序和发送程序完成。先由接收程序发送协商字符，协商校验方式，协商通过之后发送程序就开始发送数据包，接收程序接收到完整的一个数据包之后按照协商的方式对数据包进行校验，校验通过之后发送确认字符，然后发送程序继续发送下一包；如果校验失败，则发送否认字符，发送程序重传此数据包。

VRP 提供 XModem 接收程序功能，可以应用在 AUX 接口上，支持 128 字节大小的数据包和 CRC 校验。发送程序的功能自动包含在超级终端中。该协议可以用来升级 Boot ROM 程序、VRP 程序及配置文件。

⚠ 注意：

仅支持在 AUX 口上实现该功能，不支持其它的异步串口。
不支持多用户的同时操作。

4.4.1 XModem 协议配置

请在用户视图下进行下列操作。

表4-14 用 XModem 获取文件

操作	命令
用 XModem 获取文件	**xmodem get** *filename*

⚠ 注意：

filename 要求使用绝对路径名。
在升级 Boot ROM 程序、VRP 程序及配置文件时，应将 *filename* 配置为相应的文件名（可以通过 **dir** 命令查看一下当前系统中的文件名），对已经存在的同名文件，覆盖前会给出提示信息。

4.5 配置文件管理

4.5.1 简介

1. 配置文件内容及格式

配置文件为一文本文件，其格式如下：

- 以命令格式保存。
- 为了节省空间，只保存非缺省的参数（各配置参数的缺省值详见以后各章节）。
- 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）。空行或注释行可以是一行或多行。
- 节的顺序安排通常为：全局配置、物理接口配置、逻辑接口配置、路由协议配置等。
- 以 return 为结束。

2. 查看路由器配置

使用 **save** 命令保存的路由器配置以文件形式存放在 Flash 之中，路由器启动时，根据从 Flash 中读取的配置文件进行路由器的初始化工作，因此，该配置文件中的配置称为起始配置。运行过程中，路由器正在使用的配置称为当前配置，当前配置存放在路由器的内存之中，在路由器重启之后就会丢失。

请在任何视图下，进行下列操作。

表4-15 查看路由器配置

操作	命令
查看路由器的起始配置	**display saved-configuration**
查看系统保存的用于启动的配置文件	**display startup**
查看当前视图的配置	**display this**
查看路由器的当前配置	**display current-configuration**[**controller** | **interface** *interface-type* [*interface-number*] | **configuration** [**isp** | **luser** | **radius-template** | **system** | **user-interface|**]] [**|** [**begin** | **include** | **exclude**] *string*]

📖 说明：

配置文件的显示格式与保存格式相同。

3. 保存当前配置

通过命令行接口，用户可以修改路由器当前配置。为了使当前配置能够作为路由器下次上电时的起始配置，需要用 **save** 命令保存当前配置到 Flash 中，形成配置文件。

请在所有视图下进行下列操作。

表4-16 保存当前配置

操作	命令
保存当前配置	**save** [*file-name*] [**safely**]

不带 safely 参数表示快速保存配置文件，保存过程中不能对设备进行重启动、断电等。否则，会丢失配置文件。带有 safely 参数，保存配置文件的速度会慢一点。但是，如果保存过程中出现设备重启动，断电等问题，配置文件会在 Flash 中一直保存，不会丢失。

缺省方式下，采用快速保存模式。对于电源稳定程度较好的环境，推荐使用默认的快速模式。对于电源环境恶劣，或者远程维护等情况，推荐使用带有 safely 参数的保存配置命令。

📖 说明：

为了保证路由器重启之后能够使用与当前相同的配置，在重启路由器之前，建议用户使用 **save** 命令保存配置。

---

4. 擦除配置文件

用 **reset saved-configuration** 命令可以擦除路由器 Flash 中的配置文件，配置文件被擦除后，路由器下次上电时将采用缺省的配置参数进行初始化，以下几种情况时，需要擦除存储设备中的配置文件：

- 在路由器软件升级之后，可能会引起路由器软件和配置文件不匹配。
- 发现配置文件遭到破坏，如加载了错误的配置文件。

擦除配置文件后，可用 **save** 命令保存当前配置为新的配置文件。

请在用户视图下进行下列操作。

表4-17 擦除存储设备中的配置文件

操作	命令
擦除中配置文件	**reset saved-configuration**

5. 设置系统下次启动时使用的配置文件

表4-18 设置系统下次启动时使用的配置文件

操作	命令
设置系统下次启动时使用的配置文件	**startup saved-configuration** *filename*

4.5.2 配置文件命名及启动时的选择顺序

1. 配置文件的命名

vrpcfg.cfg：是用户保存配置的缺省文件名，名字由厂商规定，内容可由用户修改。

vrpcfg.def：是缺省的出厂配置文件名，内容由厂商规定。

vrpcfg.txt 是过去出厂的华为设备的配置文件。

2. 配置文件的选择顺序

系统启动时配置文件的选择顺序分为如下三种情况：

(1) 如果用户没有设置跳过配置文件启动，就按下面 2)、3)的顺序进行选择；否则，以空配置启动：

(2) 如果用户指定了启动的配置文件,则按下面的顺序进行选择；

- 若配置文件存在，则以该文件为启动配置文件。
- 若配置文件不存在，则以缺省出厂配置文件（vrpcfg.def）为启动配置文件。如果 vrpcfg.def 也不存在，以空配置启动。

(3) 如果用户不指定启动配置文件,则按下面的顺序进行选择。

- 若 vrpcfg.cfg 存在，则以 vrpcfg.cfg 为启动文件；
- 若不存在，就查找 vrpcfg.txt 文件，找到就以 vrpcfg.txt 为启动配置文件；
- 以上两个文件不存在，再查找 vrpcfg.def，找到就以 vrpcfg.def 为启动配置文件；
- 否则以空配置启动。

4.5.3 备份配置文件

配置文件可以通过以下三种方法备份下来：

- 备份 display current-configuration 命令显示。
- 通过 FTP 备份。
- 通过 TFTP 备份

1. 备份 current-configuration 命令显示

使用 **display current-configuration** 命令可以显示路由器的所有配置（缺省配置除外）。在超级终端中，拷贝其中所有的配置显示内容到一个文本文件中，就可以备份配置文件。

2. 通过 FTP 备份

通过 FTP 备份配置文件有两种方法：

一是路由器作为 FTP Server，将路由器上的配置文件下载到 PC（FTP Client）上。

路由器启动后，进行如下配置：

```
[Quidway] local-user quidway
[Quidway-luser-quidway] password simple huawei
[Quidway-luser-quidway] service-type ftp ftp-directory flash:/ftp/quidway
```

然后在已经与路由器连通的 PC 上建立到路由器的 FTP 连接，并备份配置文件：

```
C:\>ftp x.x.x.x
<ftp> get remotefile [localfile]
200 Port command okay.
150 Server okay , now transmit file .
226 file transmit success.
ftp: 735 bytes received in 0.06Seconds 12.25Kbytes/sec.
```

其中 *remotefile* 文件为路由器上的配置文件（vrpcfg.cfg）。

二是路由器作为 FTP Client，将路由器中的配置文件上传到 PC（FTP Server）中。

在已经与路由器连通的 PC 上启动 FTP Server 并配置授权信息，然后在路由器上执行如下命令：

```
<Quidway> ftp x.x.x.x
[ftp] put localfile [ remotefile ]
```

其中 *localfile* 文件应为路由器上的配置文件（vrpcfg.cfg）。

3. 通过 TFTP 备份

路由器作为 TFTP Client，将路由器上的配置文件上传到 PC（TFTP Server）上。在路由器上执行如下命令：

```
<Quidway> tftp x.x.x.x put localfile  [remotefile]
```

其中 *localfile* 文件应为路由器上的配置文件，*remotefile* 为上传到 TFTP Server 后保存的配置文件名。

第5章 用户界面配置

5.1 用户界面简介

5.1.1 用户界面概述

用户界面视图（User-interface view）是与接口视图类似的视图，是系统提供的一种新的视图，用来管理那些工作在流方式下的异步物理和逻辑接口。由于这类接口常常用于对系统进行配置管理，因此，通过用户界面视图，可以达到统一管理各种用户配置的目的。

目前系统支持的配置方式有：

- Console 口本地配置。
- AUX 口本地或远程配置。
- 工作在异步方式下的串口本地或远程配置。
- Telnet 或 SSH 本地或远程登录配置。

与这些配置方式对应的是四种类型的用户界面：

- CON 口(Console)

“控制口”（Console port）是一种线设备端口，路由器提供一个 Console 口，端口类型为 EIA/TIA-232 DCE，便于我们进行配置。

- AUX 口（AUX）

“辅助端口”（Auxiliary port）也是一种线设备端口，路由器提供一个 AUX 口，端口类型为 EIA/TIA-232 DTE，通常用于通过 Modem 进行拨号访问。

- 异步方式串口（TTY）

TTY 类型的用户界面，是指通过异步串口或同异步串口（工作在异步方式下）登录的方式。

- 虚拟线路（VTY）

“虚拟连接”（Virtual port）属于逻辑终端线，用于对路由器进行 Telnet 访问，通常简称为 VTY。

5.1.2 用户界面的编号

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

系统的用户界面共分 4 类，并按照一定的先后顺序排列：

- 分别是控制台（CON）、异步接口（TTY）、辅助接口（AUX）、虚拟接口（VTY）四种类型。控制台和辅助接口分别只有一个；TTY 和 VTY 类型的用户界面可能有多个，而每种类型的多个用户界面内部又按照顺序排列。绝对编号的起始编号是 ui0（即 CON 口），其它接口依次类推。CON、AUX 口各占一个编号；TTY、VTY 接口，不同产品可以支持的数量不同，请使用 **display user-interface** 查看即可得知。绝对编号可以唯一的指定一个用户界面或一组用户界面。

2. 相对编号方式

相对编号方式的形式是：“用户界面类型”＋“编号”。此编号是每种类型的用户界面的内部编号。此种编号方式只能指定某中类型的用户界面中的一个或一组，而不能跨类型操作。相对编号方式遵守的规则如下：

- 控制台的编号：con 0；
- 辅助线的编号：aux 0；
- TTY 的编号：第一条为 TTY 0，第二条为 TTY 1，依此类推；
- VTY 的编号：第一条为 VTY 0，第二条为 VTY 1，依此类推。

5.2 用户界面配置步骤

用户界面配置包括：

- 进入 User-interface 视图
- 配置用户界面支持的协议
- 配置异步接口属性
- 配置终端属性
- 用户管理
- Modem 属性设置
- 配置自动执行命令
- 配置 VTY 类型用户界面的呼入/呼出限制

5.2.1 进入用户界面视图

在系统视图下，键入相应的命令，即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 User-interface 进行配置，也可以进入多条用户界面视图，同时配置多条 User-interface。

表5-1 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-keyword*] *number* [*ending-number*]

进入 User-interface aux 口视图。

```
[Quidway] User-interface aux 0
[Quidway-ui-aux0]
```

在用户界面视图下，可以配置和管理各个异步口的属性，包括：

(1) 异步属性：速率（speed），流控方式（flowcontrol），校验（parity），停止位（stopbits），数据位（databits）。

(2) 终端属性配置：使能终端服务功能（shell），终端用户超时断开设定（idle-timeout），设置终端屏幕的一屏长度（screen-length），验证配置，设置历史命令缓冲区大小。

(3) 优先级设置：设置通过用户界面登录系统的用户的优先级。

(4) Modem 属性配置：Modem 和脚本配置。

5.2.2 设置所在用户界面支持的协议

该配置任务用来指定所在的用户界面支持的协议，缺省为支持所有协议，包括 PAD、Telnet 和 SSH。

请在 VTY 类型的用户界面视图下进行下列配置。

表5-2 设置所在用户界面支持的协议

操作	命令
设置所在用户界面支持的协议	**protocol inbound** { **all** | **ssh** | **telnet** | **pad** }

5.2.3 配置异步接口属性

在用户界面视图下，可以配置其异步属性。这些配置命令都只有工作在异步流方式下才有效。

请在用户界面视图下进行下列配置。

1. 配置传输速率

表5-3 配置传输速率

操作	命令
设置传输速率	**speed** *speed-value*
恢复传输速率的缺省值	**undo speed**

异步串口支持的传输速率有：

- 300bps
- 600bps
- 1200bps
- 2400bps
- 4800bps
- 9600bps
- 19200bps
- 38400bps
- 57600bps
- 115200bps
- 4096000bps

缺省的异步串口传输速率为 9600bps。实际情况下能够支持的最大速率与所使用的接口有关，如 Console 口的最大速率为 115200bps，达不到 4096000bps。

2. 配置流控方式

表5-4 配置流控方式

操作	命令
配置流控方式	**flow-control** { **none** | **software** | **hardware** }
恢复流控方式为缺省方式	**undo flow-control**

TTY 口缺省的流控方式为硬件流控。

参数说明如下：

none：不进行流控。

software：进行软件流控。

hardware：进行硬件流控，只对 AUX 口和异步方式串口有效。

3. 设置校验位

表5-5 设置校验位

操作	命令
设置校验位	**parity** { **none** | **even** | **odd** | **mark** | **space** }
设置校验位为缺省值	**undo parity**

参数说明如下：

none：无校验。

even：进行偶校验。

odd：进行奇校验。

mark：进行 mark 校验。

space：进行 space 校验。

缺省为 **none**，不进行校验。

4. 设置停止位

表5-6 设置停止位

操作	命令
设置停止位	**stopbits** { **1.5 | 1 | 2** }
恢复停止位为缺省值	**undo stopbits**

停止位的缺省值是 1。

5. 设置数据位

表5-7 设置数据位

操作	命令
设置数据位	**databits** { **5** | **6** | **7** | **8** }
恢复数据位为缺省值	**undo databits**

异步口支持的数据位为：5，6，7，8。

缺省为 8 位数据位。

5.2.4 配置终端属性

请在用户界面视图下进行下列配置。

1. 启动终端服务功能

表5-8 启动终端服务功能

操作	命令
启动终端服务	**shell**
禁止终端服务	**undo shell**

⚠ 注意：

缺省在所有的用户界面上启动终端服务。

例如：

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] undo shell
```

对于已经登陆上来的 telnet 用户没有影响，而新发起的 Telnet 连接将无法建立。

2. 终端用户超时断开设定

表5-9 设置终端用户超时断开功能

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

缺省为启动终端用户定时断开功能，时间为 10 分钟。也就是说，如果 10 分钟没有操作，此终端线路自动断开。用户可以配置 **idle-timeout 0**，即关闭定时断开功能。

3. 配置锁住用户界面

该配置用来锁住当前使用的终端线路，并提示您输入密码。防止当您离开时，其它人对该终端线路进行操作。

表5-10 锁住用户界面

操作	命令
配置锁住用户界面	**lock**

#当前以 VTY 1 线路登录路由器，有事要离开，需要锁住 user-interface vty 1:

```
<Quidway> lock
Password:xxxx
Again:xxxx
```

4. 设置终端屏幕的一屏长度

表5-11 设置终端屏幕的一屏长度

操作	命令
设置终端屏幕的一屏长度	**screen-length** *screen-length*
恢复终端屏幕一屏长度的缺省设置	**undo screen-length**

终端屏幕一屏长度的缺省为 24 行。

screen-length 0 表示关闭分屏功能。

undo screen-length 表示恢复缺省设置。

5. 设置历史命令缓冲区大小

表5-12 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** *size-value*
恢复历史命令缓冲区大小为缺省值	**undo history-command max-size**

size-value 为历史缓冲区大小。缺省值为 10，意味着缺省可存放 10 条历史命令。

6. 配置用户界面之间传递消息

send 用来实现用户界面之间传递消息。

表5-13 配置在用户界面之间传递消息

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

5.2.5 Modem 属性配置

在异步口通过 **modem** 拨入，通过用户界面视图可管理和配置 **modem** 的有关参数，相关配置命令只对 AUX 口及异步方式工作的串口有效。

表5-14 modem 配置

操作	命令
设置系统收到了 RING 信号到等待 CD_UP 的时间间隔	**modem timer answer** *seconds*
恢复系统缺省的收到 RING 信号到等待 CD_UP 的时间间隔	**undo modem timer answer**
设置自动应答	**modem auto-answer**

操作	命令
设置手动应答	**undo modem auto-answer**
设置呼入呼出开关	**modem** [**call-in** | **call-out** | **both**]
设置禁止呼入呼出	**undo modem** [**call-in** | **call-out** | **both**]

在 **aux** 口设置 **modem** 自动应答。

```
[Quidway-ui-aux0] modem auto-answer
```

5.2.6 配置自动执行命令

auto-execute command 命令使用时有如下的限制：

- Console 口不支持 **auto-execute command**。
- 如果路由器上只有一个 AUX 口，没有 Console 口（Console 口和 AUX 口共用），则此 AUX 口也不支持 **auto-execute command**。
- 对其他类型的接口不做限制。

用户在登录时，自动执行某条在该终端上用 **auto-execute command** 配置好的命令，命令执行结束后，自动断开用户线。

通常的用法是，在终端用 **auto-execute command** 配置 Telnet 命令，使用户自动连接到指定的主机。

⚠ 注意：

使用该命令后，将导致不能通过该终端线对本系统进行常规配置，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，要确保可以通过其他手段登录系统，以去掉此配置。

请在用户界面视图下进行下列配置。

表5-15 设置自动执行命令

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

配置自动执行命令后，在用户重新登录时，自动执行此命令。

用户登录后，实现自动执行 **telnet** 命令，登录到目的主机。

执行步骤为：

(1) 在用户界面视图下，执行 auto-execute command 命令。

```
[Quidway-ui4] auto-execute command telnet 10.110.100.1
```

(2) 退出系统视图，重新登录，自动执行 telnet 10.110.100.1 命令。

5.2.7 配置 VTY 类型用户界面的呼入呼出限制

该配置通过引用 ACL 控制列表，对 VTY（Telnet）类型的用户界面的呼入/呼出权限进行限制。

请在用户界面视图下进行下列配置。

表5-16 配置 VTY 类型用户界面的呼入呼出限制

操作	命令
配置 VTY 类型用户界面的呼入/呼出限制	**acl** *acl-number* { **inbound** | **outbound** }
取消 VTY 类型用户界面的呼入/呼出限制	**undo acl** { **inbound** | **outbound** }

5.3 用户界面的显示和调试

5.3.1 显示用户界面的使用信息

请在任何视图下进行下列操作。

表5-17 显示每个用户界面的用户使用信息

操作	命令
显示用户界面的使用信息	**display users** [**all**]

5.3.2 显示用户界面的物理属性和一些配置

请在任何视图下进行下列操作。

表5-18 显示用户界面的物理属性和一些配置

操作	命令
显示用户界面的物理属性和一些配置	**display user-interface** [*type-name*] [*number*]

第6章 用户管理

6.1 用户管理概述

第一次启动路由器时，路由器没有设置用户名和口令。在不对登录用户进行验证的情况下，只要将计算机终端通过 Console 口与路由器连接，任何用户可以对路由器进行配置；如果配置了主控板或接口板的 IP 地址，任何远端用户可能使用 Telnet 登录到路由器；远端用户还可能与路由器建立 PPP 连接从而访问网络。这显然对路由器和网络是不安全的。为此需要为路由器创建用户，并为用户设置口令，对用户进行管理。

📖 说明：

本章侧重于阐述 Terminal 用户及 Telnet 用户的认证管理，其他用户及 AAA Radius/HWTACACS 认证方面的内容请参见《VRP3.4 操作手册》安全部分。

6.1.1 用户分类

从用户所获得的服务来划分，可以将路由器的用户划分为：

- Terminal 用户，通过 Console 口或 Aux 口、异步口登录到路由器；
- Telnet 用户，使用 Telnet 命令登录到路由器；
- FTP 用户，与路由器建立 FTP 连接进行文件传输；
- PPP 用户，与路由器建立 PPP 连接（例如拨号、PPPoA 等），从而访问网络；
- SSH 用户，与路由器建立 SSH 连接，登录到路由器；
- PAD 用户，与路由器建立 PAD 连接，从而访问网络。

一个用户可能同时获得几种服务，这样只需一个用户便可以执行多种功能。

6.1.2 用户的优先级

系统可以对超级终端用户和 Telnet 用户进行分级管理。与命令的优先级一样，用户的优先级分为参观（Visit）、监控（Monitor）、系统（System）、管理（Manage）4 个级别，级别标识为 0～3。用户所能访问命令的级别，由用户的级别确定。如果不对用户进行认证或采用 password 认证的情况下，登录到路由器的用户所能访问的命令级别由登录所使用的用户界面的级别确定。

用户所能访问的命令包括用户级别的命令以及低于用户级别的命令，例如用户的级别为 2，则用户可以访问级别为 0、1、2 的命令。级别为 3 的用户可以访问所有的命令。各级别用户所能访问的命令如表 6-1所示。

表6-1 用户优先级

用户级别	名称	所能访问的命令
0	参观	**ping、tracert、telnet、super、language-mode 、quit**
1	监控	0 级命令、**msdp-tracert、mtracert、reboot、reset、send、terminal、undo、upgrade、display、debugging**
2	系统	所有配置命令（管理级的命令除外）和 0、1 级命令
3	管理	所有命令

📖 说明：

管理级的命令是指文件系统命令、FTP 命令、TFTP 命令。

6.1.3 认证方案

用户登录路由器时，系统会对用户的身份进行认证。对用户的认证有 4 种方案：不认证、password 认证、本地认证、AAA 服务器认证。不认证即不需用户名和口令，就可登录路由器。为安全起见，不认证方案是不可取的。password 认证只需口令，不需用户名，可以获得一定的安全性。本地认证需要用户提供用户名和口令，该用户名和口令必须与路由器上的配置保持一致；AAA 服务器认证也需要用户提供用户名和口令，该用户名和密码必须与 AAA 服务器上配置的一致，拨号用户常采用这种认证方案。

对 Telnet 用户和 Terminal 用户一般采用本地认证。

6.1.4 规划路由器的用户

可以根据需要规划路由器的用户。通常，路由器至少需要创建一个超级终端用户——Console 用户。如果需要从远端使用 Telnet 登录到路由器，则需配置一个 Telnet 用户。为了让远端用户向路由器加载或下载文件，可以配置 FTP 用户。为了让用户通过与路由器建立的 PPP 连接访问网络，则需要配置 PPP 用户。

本章主要介绍如何配置 Telnet 用户和超级终端用户。FTP 用户的配置请参考本模块的《文件管理》中的 FTP 配置的内容。PPP 用户的配置请参考本手册《链路层协议》及《安全》模块的内容。

6.2 配置用户

配置用户的任务包括：

- 配置认证用户的方式
- 配置用户名及口令
- 设置用户优先级

认证用户的作用是使合法用户能登录并使用路由器，非法用户不能通过认证而不能使用路由器。

6.2.1 配置认证用户的方式

配置认证用户的方式是用来设置指定用户登录路由器时所需的认证方法。

请在用户界面视图下，执行如下的命令：

表6-2 配置认证用户的方式

操作	命令
设置进行用户认证	**authentication-mode** { **password** | **scheme** [**command-authorization**] }
设置不进行用户认证	**authentication-mode none**

关键字 **none** 表示不认证用户身份。关键字 **password** 表示认证不需用户名，只需口令字。**scheme** 表示使用 AAA 配置的认证方案进行认证（包括本地认证方案和 RADIUS、HWTACACS 认证，具体认证方案由 **scheme** 命令来指定）。

TTY（即异步接口用户）、VTY 类型（即 Telnet、SSH、PAD 用户）、AUX 的用户界面缺省为 **password** 方式认证，其它类型用户界面缺省不进行终端认证。

在配置 Telnet 用户和 Teminal 用户的认证方式时，通常设置为 **scheme** 方式中的本地认证方案。

scheme 认证方式请参考《VRP3.4 操作手册》安全部分。

6.2.2 配置用户名及口令

1. 设置 password 方式认证的口令

如果在配置认证方式时选择 **password** 方式进行用户认证，则需设置 password 认证的口令。

请在用户界面视图下进行如下配置。

表6-3 设置 password 认证的口令

操作	命令
设置 password 认证的口令	**set authentication password** { **cipher** | **simple** } *password*
取消 password 认证的口令	**undo set authentication password**

cipher 表示配置密文密码，**simple** 表示配置明文密码。

2. 设置进行本地认证的用户名和口令

如果选择本地认证，则需先设置用户名和口令。

表6-4 配置进行 AAA 本地认证的用户名及口令

操作	命令
配置用户（系统视图）	**local-user** *user-name*
取消用户（系统视图）	**undo local-user** { *user-name* **| all** }
设置本地用户的密码（本地用户视图）	**password { cipher | simple }** *password*
取消本地用户的密码（本地用户视图）	**undo password**

cipher 表示配置密文密码，**simple** 表示配置明文密码。

然后配置用户使用本地认证方案。

表6-5 配置域用户使用本地认证方案

操作	命令
创建一个 ISP 域，或者进入已创建 ISP 域的视图 （系统视图）	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }
删除指定的 ISP 域。（系统视图）	**undo domain** *isp-name*
配置当前 ISP 域用户使用本地认证方案（ISP 域视图）	**scheme local**

6.2.3 设置用户的优先级

用户所能访问的系统命令可以从两方面进行限制，一个是用户界面的优先级，一个是用户的优先级。

1. 设置用户界面的优先级

本命令可以设置各用户界面的优先级。

请在用户界面视图下进行下列配置。

表6-6 设置用户界面的优先级

操作	命令
设置用户界面的优先级	user privilege level *level*
恢复用户界面缺省的优先级	undo user privilege level

CON 口对应的优先级缺省为 3，其它用户界面的优先级缺省为 0。

例如，设置 CON 口的优先级为 3，从 VTY 0 的优先级为 2。

```
[Quidway-ui-console0] user privilege level 3
[Quidway-ui-vty0] user privilege level 2
```

这样当同一个用户分别从 CON 口和 VTY 0 登录时，其所能访问的命令是不同的（假设从这 2 个用户界面登录时均不需要认证）。当他从 CON 口登录时，可以使用所有的命令；但当他从 VTY 0 登录时，只能访问 2 级以下的命令。

2. 设置用户的优先级

本命令可以根据用户名来配置指定用户的优先级。

请在本地用户视图下进行下列配置。

表6-7 设置用户优先级

操作	命令
设置用户优先级	**level** *level*
恢复用户优先级的默认值	**undo level**

level 代表用户的优先级，其范围是 0～3。0 级别最低，3 级别最高。在配置用户以后，用户默认的优先级为 1。

📖 说明：

如果配置的认证方式为不认证或采用 password 认证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。如果配置的认证方式需要用户名和口令，则用户登录系统后所能访问的命令级别由用户的优先级确定。

6.3 显示用户信息

在配置了用户账号后，可以使用下面的命令显示所配置的用户、本地用户以及在线用户信息。

请在所有视图下进行下列操作。

表6-8 显示用户信息

操作	命令
显示用户界面的使用信息	**display users** [**all**]
查看本地用户列表	**display local-user**
查看在线用户	**display aaa user**

6.4 用户管理举例

6.4.1 使用 password 方式认证用户

要求对从 VTY 0 登录的用户进行 password 认证，用户登录时需要输入口令 huawei 才能登录成功，用户优先级为 3。操作命令如下：

```
<Quidway> system-view
[Quidway] user-interface vty 0
[Quidway-ui-vty0] authentication-mode password
[Quidway-ui-vty0] set authentication password simple huawei
[Quidway-ui-vty0] user privilege level 3
```

6.4.2 使用本地用户数据库进行用户认证

要求用户从 VTY 0 登录时输入已配置的用户名 vrp 和对应的口令 huawei，用户名和口令正确才能登录成功。操作命令如下：

```
<Quidway> system-view
[Quidway] user-interface vty 0
[Quidway-ui-vty0] authentication-mode scheme
[Quidway-ui-vty0] quit
[Quidway] local-user vrp
[Quidway-luser-vrp]password simple huawei
[Quidway-luser-vrp]service-type telnet
[Quidway-luser-vrp]level 3
[Quidway] domain system
[Quidway-isp-system] scheme local
```

第7章 NTP 配置

7.1 NTP 协议简介

网络时间协议（Network Time Protocol，简称 NTP）是用来在整个网络内发布精确时间的 TCP/IP 协议，其本身的传输基于 UDP。其基本原理如下：

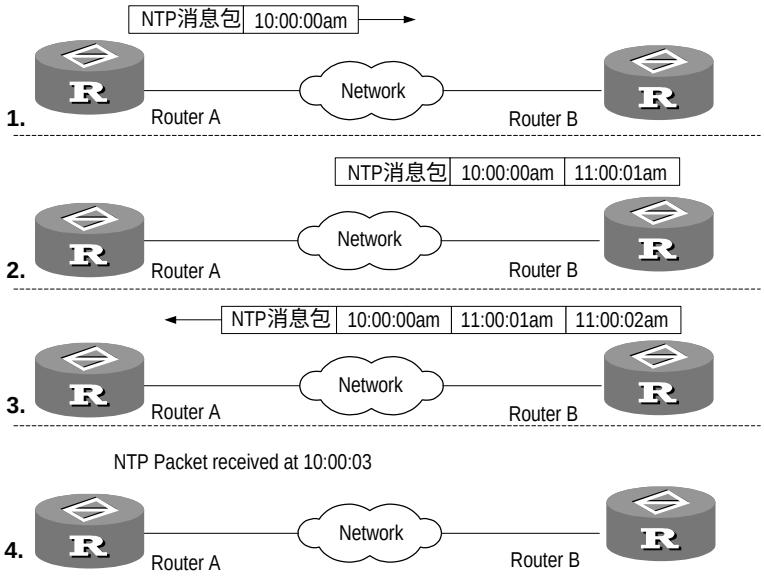

图7-1 NTP 基本原理图

上图所示的是 NTP 基本工作原理，路由器 A 和路由器 B 通过网络相连，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：

- 在路由器 A 和 B 的系统时钟同步之前，路由器 A 的时钟设定为 10:00:00am，路由器 B 的时钟设定为 11:00:00am。
- 以路由器 B 为 NTP 时间服务器，即路由器 A 将使自己的时钟与路由器 B 的时钟同步。
- 数据包在路由器 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：

- 路由器 A 发送一个 NTP 消息包给路由器 B，该消息包带有它离开路由器 A 时的时间戳，该时间戳为 10:00:00am（T_1）。
- 当此 NTP 消息包到达路由器 B 时，路由器 B 加上自己的时间戳，该时间戳为 11:00:01am（T_2）。

- 当此 NTP 消息包离开路由器 B 时，路由器 B 再加上自己的时间戳，该时间戳为 11:00:02am（T_3）。
- 当路由器 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，路由器 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）。
- 路由器 A 相对路由器 B 的时间差 offset=（（T_2-T_1）+（T_3-T_4））/2。

这样，路由器 A 就能够根据这些信息，来设定自己的时钟，使之与路由器 B 的时钟同步。

这只是 NTP 工作原理的一个粗略描述，在 RFC1305 规范中，NTP 使用复杂的算法，来确保时钟同步的精确性。

根据网络结构以及路由器在网络中的位置， NTP 有六种工作模式。

- 设置远程服务器为本地时间服务器，此时本地路由器工作在 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；
- 设置远程服务器作为本地路由器的对等体，本地运行在 symmetric active 模式（即主动模式）在。这种配置下，本地服务器能同步到远程服务器（被动模式），远程服务器也能同步到本地服务器。如果双方都有参考时钟，以层数小的为准；
- 设置本地路由器的一个接口发送 NTP 的广播消息包，此时，本地路由器工作在广播服务器模式；
- 设置本地路由器的一个接口接收 NTP 的广播信息包，此时，本地路由器工作在广播客户模式；
- 设置本地路由器的一个接口发送 NTP 组播消息包，本地路由器运行在组播服务器模式；
- 设置本地路由器的一个接口接收 NTP 组播消息包，本地路由器运行在组播客户模式。

前两种模式，也即单播模式，支持 NTP 多实例，可以实现 MPLS VPN 网络的时间同步，即物理位置不同的网络设备（CE、PE），只要属于同一个 VPN，就可以通过 MPLS VPN 相连来获得时间同步。具体功能如下：

- CE 上 的 NTP Client 可以同步到 PE 上 NTP Server；
- PE 上的 NTP Client 可以通过指定的 VPN 实例同步到 CE 上的 NTP Server；
- PE 上的 NTP Server 可以支持同步多个不同 CE 上的 NTP Client。

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
- 设置本地路由器和 NTP 广播服务器之间的往返延迟
- 设置 NTP 身份验证功能
- 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
- 设置对本地路由器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

根据网络结构以及路由器在网络中的位置，可设置六种 NTP 工作模式。

- 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

1. 配置 NTP 服务器模式

设置以 *X.X.X.X* 或 *server-name* 所指定的远程服务器作为本地时间服务器。*X.X.X.X* 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。本地路由器工作在 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。当在 PE 上指定了 *vpn-instance-name* 时，PE 上的 NTP 客户端通过指定的 VPN 实例可以同步 CE 上的 NTP 服务器，此时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 服务器模式

操作	命令
配置 NTP 服务器模式	**ntp-service unicast-server** [**vpn-instance** *vpn-instance-name*] { *X.X.X.X* | *server-name* } [**version** *number* | **source-interface** *interface-type interface-number* | **priority**] *
取消 NTP 服务器模式	**undo ntp-service unicast-server** { *X.X.X.X* | *server-name* }

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 1～4294967295； *interface-type interface-number* 指定一个接口，本地路由器给时间

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。

2. 配置 NTP 对等体模式

设置以 *X.X.X.X* 或 *server-name* 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。*X.X.X.X* 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，本地路由器能同步到远程服务器，远程服务器也能同步到本地服务器。当在 PE 上指定了 *vpn-instance-name* 时， PE 上的本地 NTP 服务器通过指定的 VPN 实例可以同步到 CE 上的 NTP 服务器，同时 CE 的 NTP 服务器也能同步到 PE 的 NTP 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** [**vpn-instance** *vpn-instance-name*] { *X.X.X.X* | *server-name* } [**version** *number* | **authentication-key** *keyid* | **source-interface** *interface-type interface-number* | **priority**] *
取消 NTP 对等体模式	**undo ntp-service unicast-peer** { *X.X.X.X* | *server-name* }

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 1～4294967295； *interface-type interface-number* 指定本地路由器给对等体发送 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。

3. 配置 NTP 广播服务器模式

指定本地路由器上的一个接口来发送 NTP 广播消息包，本地运行在广播服务器模式，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 1～4294967295；此命令必须在欲发送 NTP 广播消息包的接口下配置。

4. 配置 NTP 广播客户模式

指定本地路由器上的某接口来接收 NTP 广播消息包，并运行在广播客户模式。本地路由器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，本地路由器为了估计网络延迟，先启用一个短暂的 client/server 模式与远程服务器交换消息，然后，本地路由器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。

5. 配置 NTP 组播服务器模式

指定本地路由器上的一个接口来发送 NTP 组播消息包，本地运行在组播服务器模式，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** [*X.X.X.X*] [**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 1～4294967295；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。

6. 配置 NTP 组播客户模式

指定本地路由器上的接口，来接收 NTP 组播消息包，本地路由器运行在组播客户模式。本地路由器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，本地路由器为了估计网络延迟，先启用一个短暂的 client/server 模式与远程服务器交换消息，然后，本地路由器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** [*X.X.X.X*]
取消配置 NTP 组播客户模式	**undo ntp-service multicast-client**

组播 IP 地址 *X.X.X.X* 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

NTP 身份验证功能需要在 Server 端和 Client 端同时配置，保证密钥一致，并为可信密钥，验证才能通过。

1. 启动 NTP 身份验证功能

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**

2. 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。

3. 设置指定密钥是可信的

该配置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 设置指定密钥是可信的

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。

4. 将 NTP Server 与验证密钥关联

对于服务器模式和对等体模式，应在 Client 端将指定密钥与对应的 NTP Server 关联。这两种模式下，Client 端可能同时配置了多个 Server，所以需要利用认证密钥来决定同步哪一个 Server。

表7-10 将指定密钥与对应的 NTP Server 关联

操作	命令
服务器模式下，将指定密钥与对应的 NTP Server 关联	**ntp-service unicast-server** { *X.X.X.X* | *server-name* } **authentication-keyid** *keyid*
对等体模式下，将指定密钥与对应的 NTP Server 关联	**ntp-service unicast-peer** { *X.X.X.X* | *server-name* } **authentication-key** *keyid*

对于广播服务器模式和组播服务器模式，应在 Server 端将 Server 与对应的密钥关联。

表7-11 将指定密钥与对应的 NTP Server 关联

操作	命令
广播服务器模式下，将指定密钥与对应的 NTP Server 关联	**ntp-service broadcast-server authentication-keyid** *keyid*
组播服务器模式下，将指定密钥与对应的 NTP Server 关联	**ntp-service multicast-server authentication-keyid** *keyid*

7.2.3 设置本地发送 NTP 消息的接口

指定本地发送 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的。

请在系统视图下进行下列配置。

表7-12 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-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-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。

7.2.4 设置 NTP 主时钟

该配置用来设置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7-13 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** [*X.X.X.X*] [*layers-number*]
取消 NTP 主时钟设置	**undo ntp-service refclock-master** [*X.X.X.X*]

X.X.X.X 是参考时钟 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；*layers-number* 用来指定本地时钟所在的层数，范围为 1～15，缺省为 8。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。

7.2.5 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。

请在接口视图下进行下列配置。

表7-14 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/允许接收 NTP 消息的接口下配置。

7.2.6 设置对本地路由器 NTP 服务的访问控制权限

设置对本地路由器 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**、**server**、**server only (synchronization)**、**query only**。

请在系统视图下进行下列命令的操作。

表7-15 设置对本地路由器服务的访问控制权限

操作	命令
设置对本地路由器服务的访问控制权限	**ntp-service access** { **query** | **synchronization** | **server** | **peer** } *acl-number*
取消设置对本地路由器服务的访问控制权限	**undo ntp-service access** { **query** | **synchronization** | **server** | **peer** }

IP 地址访问列表标号 *acl-number* 范围为 2000～2999。其访问权限含义为：

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。

server：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。

7.2.7 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7-16 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7-17 NTP 显示与调试

操作	命令
显示 NTP 服务的状态信息	**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**
打开 NTP 的调试开关	**debugging ntp-service** { **all** | **access** | **adjustment** |**authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** }

7.4 NTP 典型配置举例

7.4.1 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

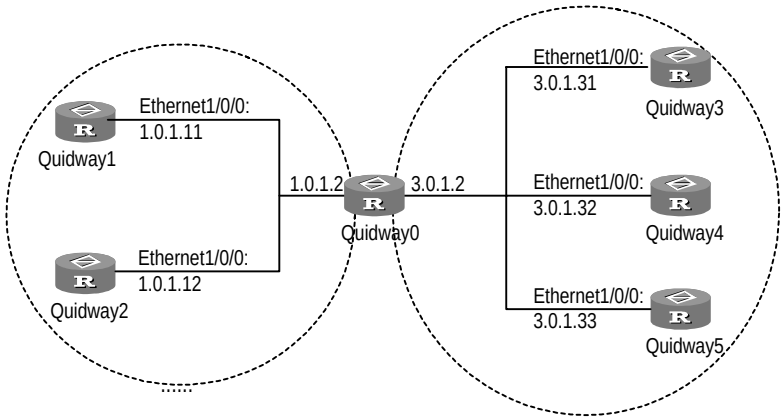

图7-2 NTP 典型配置的组网图

3. 配置步骤

(1) 配置路由器 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
```

(2) 配置路由器 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 status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 99.8562 Hz
 Actual frequency: 99.8562 Hz
 Clock precision: 2^17
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

同步后观测 Quidway2 的状态为：

```
[Quidway2] display ntp-service status
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

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
      source          refid       st  now  poll reach  delay offset   dis
**************************************************************************
[12345]127.127.7.1  LOCAL(0)    3    1    64   377    26.1    199.53  9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

7.4.2 配置 NTP 对等体举例

1. 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。

2. 组网图

如图 7-2所示。

3. 配置步骤

(1) 配置路由器 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
```

(2) 配置路由器 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
```

(3) 配置路由器 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 为对等体。

```
[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 status: synchronized
 Clock stratum: 2
 Reference clock ID: 3.0.1.33
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

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
      source          refid       st  now  poll reach  delay offset   dis
**************************************************************************
[12345]127.127.7.1  LOCAL(0)    3    1    64   377    26.1   199.53   9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

7.4.3 配置 NTP 广播模式

1. 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 Ethernet 1/0/0 向外发送广播消息包，设置 Quidway4 和 Quidway1 分别从各自的接口 Ethernet 1/0/0 监听广播消息。

2. 组网图

如图 7-2所示。

3. 配置步骤

(1) 配置路由器 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 Ethernet 1/0/0 视图。

```
[Quidway3] interface ethernet 1/0/0
```

设置为广播服务器。

```
[Quidway3-Ethernet1/0/0] ntp-service broadcast-server
```

(2) 配置路由器 Quidway4

进入系统视图。

```
<Quidway4> system-view
```

进入接口 Ethernet 1/0/0 视图。

```
[Quidway4] interface ethernet 1/0/0
[Quidway4-Ethernet1/0/0] ntp-service broadcast-client
```

(3) 配置路由器 Quidway1

进入系统视图。

```
<Quidway1> system-view
```

进入接口 Ethernet 1/0/0 视图。

```
[Quidway1] interface ethernet 1/0/0
[Quidway1-Ethernet1/0/0] ntp-service broadcast-client
```

以上配置将 Quidway4 和 Quidway1 配置为从接口 Ethernet 1/0/0 监听广播消息，而 Quidway3 从接口 Ethernet 1/0/0 发送广播消息包，由于 Quidway1 与 Quidway3 不在同一网段，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: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

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          refid       st  now  poll reach  delay offset   dis
**************************************************************************
[12345]127.127.7.1  LOCAL(0)    3    1    64   377    26.1   199.53   9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

7.4.4 配置带认证的 NTP 广播模式

1. 组网需求

Quidway3 设置本地时钟作为 NTP 主时钟，层数为 3，并从接口 Ethernet 1/0/0 向外发送广播消息包，设置 Quidway4 从接口 Ethernet 1/0/0 监听广播消息。

2. 组网图

如图 7-2所示。

3. 配置步骤

(1) 配置路由器 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 3。

```
[Quidway3] ntp-service refclock-master 3
```

启动认证功能。

```
[Quidway3] ntp-service authentication enable
```

设置 NTP 验证密钥。

```
[Quidway3] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

设置本验证密钥可信。

```
[Quidway3] ntp-service reliable authentication-keyid 88
```

进入接口 Ethernet 1/0/0 视图。

```
[Quidway3] interface ethernet 1/0/0
```

设置本路由器为 NTP 广播服务器并指定验证 ID。

```
[Quidway3-Ethernet1/0/0] ntp-service broadcast-server authentication-id 88
```

(2) 配置路由器 Quidway4

进入系统视图。

```
<Quidway4> system-view
```

启动认证功能。

```
[Quidway3] ntp-service authentication enable
```

设置 NTP 验证密钥。

```
[Quidway3] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

设置本验证密钥可信。

```
[Quidway3] ntp-service reliable authentication-keyid 88
```

进入接口 Ethernet 1/0/0 视图。

```
[Quidway4] interface ethernet 1/0/0
```

设置本路由器为 NTP 广播客户端。

```
[Quidway4-Ethernet1/0/0] ntp-service broadcast-client
```

以上配置将 Quidway4 配置为从接口 Ethernet 1/0/0 监听广播消息，而 Quidway3 从接口 Ethernet 1/0/0 发送广播消息包，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: 4
reference clock ID: 3.0.1.31
nominal frequency: 250.0000 Hz
actual frequency: 249.9992 Hz
clock precision: 2^19
clock offset: 198.7425 ms
root delay : 27.47 ms
root disper: 208.39 ms
peer disper: 9.63 ms
reference time: 17:03:32.022 UTC Sep 6 2003(BF422AE4.05AEA86C)
```

此时 Quidway4 已经与 Quidway3 同步，层数比 Quidway3 大 1，为 4。

7.4.5 配置 NTP 组播模式

1. 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 Ethernet 1/0/0 向外发送组播消息包；设置 Quidway4 和 Quidway1 分别从各自的接口 Ethernet 1/0/0 监听组播消息。

2. 组网图

如图 7-2所示。

3. 配置步骤

(1) 配置路由器 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 Ethernet 1/0/0 的视图。

```
[Quidway3] interface ethernet 1/0/0
```

设置为组播服务器。

```
[Quidway3-Ethernet1/0/0] ntp-service multicast-server
```

(2) 配置路由器 Quidway4

进入系统视图。

```
<Quidway4> system-view
```

进入接口 Ethernet 1/0/0 的视图。

```
[Quidway4] interface Ethernet 1/0/0
```

设置为组播客户模式。

```
[Quidway4-Ethernet1/0/0] ntp-service multicast-client
```

(3) 配置路由器 Quidway1

进入系统视图。

```
<Quidway1> system-view
```

进入接口 Ethernet 1/0/0 的视图。

```
[Quidway1] interface ethernet 1/0/0
```

设置为组播客户模式。

```
[Quidway1-Ethernet1/0/0] ntp-service multicast-client
```

以上配置将 Quidway4 和 Quidway1 配置为从接口 Ethernet 1/0/0 监听组播消息，而 Quidway3 从接口 Ethernet 1/0/0 发送组播消息包，由于 Quidway1 与 Quidway3 不在同一的网段，所以 Quidway4 收不到 Quidway3 发出的组播包，而 Quidway4 接收到 Quidway3 发出的组播包后与其同步。

同步后观测 Quidway4 的状态为：

```
[Quidway2] display ntp-service status
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
```

```
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 Quidway4 已经与 Quidway3 同步，层数比 Quidway3 大 1，为 3。

观察 Quidway4 的 sessions 情，Quidway4 与 Quidway3 建立了连接。

```
[Quidway4] display ntp-service sessions
      source          refid       st  now  poll reach  delay offset   dis
**************************************************************************
[12345]127.127.7.1  LOCAL(0)    3    1    64   377    26.1   199.53   9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

7.4.6 配置带身份验证的 NTP 服务器模式

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，同时加入身份验证。

2. 组网图

如图 7-2所示。

3. 配置步骤

(1) 配置路由器 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
```

(2) 配置路由器 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 authentication-keyid 42
```

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，向 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
```

此时，Quidway2 可以向 Quidway1 同步，同步后观测 Quidway2 的状态为：

```
[Quidway2] display ntp-service status
clock status: synchronized, stratum: 3, reference clock ID: 1.0.1.11
nominal freq: 250.0000 Hz, actual freq: 249.9992 Hz, precision: 2**19
offset: 198.7425 ms, reftime: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
root delay : 27.47 ms, root disper: 208.39 ms, peer disper: 9.63 ms
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

可以看出，Quidway2 已经与 Quidway1 同步，层数比 Quidway1 大 1，为 3。

第8章 SNMP 配置

8.1 协议简介

8.1.1 SNMP 协议介绍

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一项工业标准，是目前用得最广泛的计算机网络管理协议。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，对信息进行修改，寻找故障，完成故障诊断、容量规划和报告的生成。它采用轮询机制，提供最基本的功能集，适合于小型、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，受到了广泛的支持。

SNMP 的结构分为 NMS（Network Management Station）和 AGENT 两部分，NMS 是运行客户端程序的工作站，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 和 AGENT 之间通过如下方式进行消息交互。一方面，NMS 可以向 AGENT 发出 GetRequest、GetNextRequest、GetBulkRequest 和 SetRequest 请求报文，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，返回给 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。

8.1.2 SNMP 版本及支持的 MIB

设备中的管理对象在 SNMP 报文中用管理变量来描述，为了唯一标识设备中的管理对象，SNMP 用层次结构命名方案来识别管理对象。整个层次结构就象一棵树，树的节点表示管理对象，如下图所示。每一个节点，都可以用从根开始的一条路径别无二义地标识。

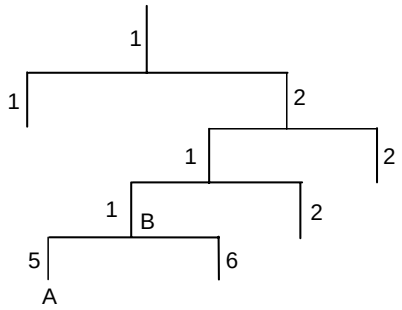

图8-1 MIB 树结构

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，路由器系统中的 SNMP Agent 支持标准网管 SNMP v3，兼容 SNMP v1、SNMP v2c。

8.2 SNMP 配置

SNMP 的配置包括：

- 启动或关闭 SNMP Agent 服务
- 使能或禁止 SNMP 协议的相应版本
- 设置团体名
- 配置一个 SNMP 的组
- 为一个 SNMP 组添加或删除用户
- 设置管理员的联系方法
- 允许/禁止发送 Trap 报文
- 设置本地设备的引擎 ID
- 设置 Trap 目标主机的地址
- 设置路由器的位置信息
- 指定发送 Trap 报文的源地址
- 创建或者更新 MIB 视图的信息
- 设置发往目的主机（host）的 Trap 报文的消息队列的长度
- 设置 Trap 报文的保存时间
- 设置 Agent 能接收/发送的 SNMP 消息包的大小

8.2.1 启动或关闭 SNMP Agent 服务

该配置任务用来启动 SNMP Agent 服务，缺省情况为关闭 SNMP Agent 服务。

请在系统视图下进行下列配置。

表8-1 启动/关闭 SNMP Agent 服务

操作	命令
启动 SNMP Agent 服务	**snmp-agent**
关闭 SNMP Agent 服务	**undo snmp-agent**

8.2.2 使能或禁止 SNMP 协议的相应版本

该配置任务用来使能 SNMP 协议的相应版本，缺省情况为使能 SNMP v3 版本。如果要使能 SNMP v1 版本、SNMP v2c 版本，需要用该命令进行设置。

请在系统视图下进行下列配置。

表8-2 使能/禁止 SNMP 相应版本

操作	命令
使能 SNMP 协议的相应版本	**snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }
禁止 SNMP 协议的相应版本	**undo snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }

*：表示从 **v1**、**v2c**、**v3** 这三个选项中选取多个，最少选取一个，最多选取所有三个选项。

使能 SNMP V2C、SNMP V3 版本。

```
[Quidway] snmp-agent sys-info version v3 v2c
```

禁止 SNMP V2C、SNMP V1 版本。

```
[Quidway] undo snmp-agent sys-info version v1 v2c
```

8.2.3 设置团体名

SNMPV1、SNMPV2C 采用团体名认证，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）或读写（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。

请在系统视图下进行下列配置。

表8-3 设置或删除团体名

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-number*]]*
取消先前设置的团体名	**undo snmp-agent community** *community-name*

对同一个团体名进行重复配置时，后配置的属性会覆盖先前配置的属性。

设置 public 团体具有只读权限。

```
[Quidway] snmp-agent community read public
```

设置 private 团体具有读写权限。

```
[Quidway] snmp-agent community write private
```

8.2.4 设置/删除 SNMP 组

该配置任务可以设置或删除 SNMP 的一个组。

请在系统视图下进行下列配置。

表8-4 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** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**acl** *acl-number*] **snmp-agent group** { **v1** | **v2c** } *group-name* **acl** *acl-number* **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* **acl** *acl-number*
删除一个 SNMP 组	**undo snmp-agent group** { **v1** | **v2c** } *group-name* **undo snmp-agent group v3** *group-name* [**authentication** | **privacy**]

snmp-agent group v3 命令在不配置视图的情况下有默认的 ViewDefault 视图，该视图是只读视图，其他的视图需要配置。

snmp-agent group { **v1** | **v2c** } 实际上是配置 SNMP 的团体属性。缺省情况下，与 **snmp-agent group v3** 相同。

8.2.5 添加/删除用户

该配置任务用来为一个 SNMP 的组添加或删除一个用户。

请在系统视图下进行下列配置。

表8-5 为 SNMP 组添加一个新用户或删除一个用户

操作	命令
为一个 SNMP 组添加一个新用户	**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 des56** *priv-password*]] [**acl** *acl-number*]
删除 SNMP 组的一个用户	**undo snmp-agent user** { **v1** | **v2c** } *user-name group-name* **undo snmp-agent user v3** *user-name group-name* [**engineid** *engine-id* | **local**]

为 SNMP 组 Johngroup 加入一个用户 John，安全级别为需要认证、指定认证协议为 HMAC-MD5-96、认证密码为 hello。

```
[Quidway] snmp-agent usm-user v3 John Johngroup authentication-mode md5 hello
```

8.2.6 设置管理员的联系方法

设置管理员的联系方法（system contact）是 MIB II 中 system 组的一个管理变量，内容为被管理设备（路由器）相关人员的标识及联系方法。您可以通过设置此参数，将重要信息存储在路由器中，以便出现紧急问题时查询使用。

请在系统视图下进行下列配置。

表8-6 设置或删除管理员的联系方法

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**

例：

```
[Quidway] snmp-agent sys-info contact Mr.zhang 13800138002
```

8.2.7 允许/禁止发送 Trap 报文

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。

请在系统视图下进行下列配置。

表8-7 允许或禁止发送 Trap 报文

操作	命令
允许发送 Trap 报文	**snmp-agent trap enable** [*trap-type* [*trap-list*]]
禁止发送 Trap 报文	**undo snmp-agent trap enable** [*trap-type* [*trap-list*]]

缺省为允许发送 Trap 报文。

snmp-agent trap enable 命令不带参数时，表示允许发送所有模块的所有类型的 Trap 报文。

8.2.8 设置本地设备的引擎 ID

该配置任务可以设置本地设备的引擎 ID。引擎 ID 是十六进制数字串，并且长度为 10～64 个十六进制数，缺省为公司的企业号+设备信息。设备信息可以是 IP 地址、MAC 地址或自己定义的十六进制数字串。

请在系统视图下进行下列配置。

表8-8 设置本地设备的引擎 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**

8.2.9 设置 Trap 目标主机的地址

请在系统视图下进行下列配置。

表8-9 设置或取消 Trap 目标主机的地址

操作	命令
设置 Trap 主机的地址	**snmp-agent target-host trap address udp-domain** *X.X.X.X* [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** { **authentication** | **privacy** }]
取消 Trap 主机的地址	**undo snmp-agent target-host** *X.X.X.X* **securityname** *security-string*

例：允许向地址 202.38.160.6 发送 Trap 报文，使用的团体名为 public。

```
[Quidway] snmp-agent target-host trap address udp-domain 202.38.160.6
udp-port 5000 params securityname public
```

8.2.10 设置路由器的位置信息

路由器的位置信息是 MIB 中 system 组的一个管理变量，用于表示被管理设备的位置。

请在系统视图下进行下列配置。

表8-10 设置路由器的位置信息

操作	命令
设置路由器位置	**snmp-agent sys-info location** *sysLocation*
恢复路由器位置为缺省值	**undo snmp-agent sys-info location**

例：将路由器的位置信息设为 hwbj。

```
[Quidway] snmp-agent sys-info location hwbj
```

8.2.11 指定发送 Trap 的源地址

该配置任务可以设定或删除发送 Trap 的源地址。

请在系统视图下进行下列配置。

表8-11 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-type interface-number* [subinterface-type]
取消发送 Trap 的源地址	**undo snmp-agent trap source**

例：将以太网接口 1/0/0 的 IP 地址作为 Trap 报文的源地址。

```
[Quidway] snmp-agent trap source ethernet 1/0/0
```

8.2.12 MIB 视图信息设置

该配置任务可以创建、更新或者删除视图的信息。

请在系统视图下进行下列配置。

表8-12 创建或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*

例：创建一个视图包含 internet (1.3.6.1)的所有对象。

```
[Quidway] snmp-agent mib-view included myview 1.3.6.1
```

8.2.13 设置消息包的最大值

该配置任务可以设置 Agent 能接收/发送的 SNMP 消息包的最大值。

请在系统视图下进行下列配置。

表8-13 设置 Agent 接收/发送的 SNMP 消息包的最大值

操作	命令
设置 Agent 接收/发送的 SNMP 消息包的最大值	**snmp-agent packet max-size** *byte-count*
恢复 SNMP 消息包的最大值的缺省值	**undo snmp-agent packet max-size**

Agent 能接收/发送的 SNMP 消息包的最大值的取值范围为<484-17940>，单位为字节，缺省值为 1500 字节。

设置 Agent 能接收/发送的 SNMP 消息包的最大值为 1042 字节。

```
[Quidway] snmp-agent packet max-size 1042
```

8.2.14 设置 Trap 报文的消息队列的长度

该配置任务可以设置发往目的主机（host）的 Trap 报文的消息队列的长度。

请在系统视图下进行下列配置。

表8-14 设置 Trap 报文的消息队列的长度

操作	命令
设置发往目的主机（host）的 Trap 报文的消息队列的长度	**snmp-agent trap queue-size** *size*
恢复消息队列长度的缺省值	**undo snmp-agent trap queue-size**

消息队列长度的取值范围为<1-1000>，缺省值为 100。

设置发送 Trap 报文的主机的消息队列的长度为 200。

```
[Quidway] snmp-agent trap queue-size 200
```

8.2.15 设置 Trap 报文的保存时间

该配置任务用来设置 Trap 报文的保存时间，超过该时间的 Trap 报文将被丢弃。

请在系统视图下进行下列配置。

表8-15 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**

seconds 取值范围为<1～2592000>，缺省值为 120 秒。

设置 Trap 报文的保存时间为 60 秒。

```
[Quidway] snmp-agent trap life 60
```

8.3 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，均可以显示配置后 SNMP 的运行情况，通过查看显示信息，来验证配置的效果。

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

表8-16 SNMP 的显示与调试

操作	命令
显示 SNMP 使能的版本信息	**display snmp-agent sys-info version**
显示 SNMP 报文统计信息	**display snmp-agent statistics**
显示当前设备的引擎 ID	**display snmp-agent** { **local-engineid** | **remote-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。	**display snmp-agent group** [*group-name*]
显示组用户名表中所有 SNMP 用户名称的信息	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*] *
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** *view-name*]
显示系统维护联络信息字符串	**display snmp-agent sys-info contact**
显示系统位置字符串	**display snmp-agent sys-info location**
打开 SNMP 调试开关	**debugging snmp-agent** { **header** | **packets** | **trap** | **process** }

8.4 SNMP 典型配置举例

1. 组网需求

以下图为例，网管工作站（NMS）与路由器通过以太网相连，网管工作站 IP 地址为 129.102.149.23，路由器以太网口 IP 地址为 129.102.0.1。NMS 接收 trap 的端口号为 5000，SNMP 的版本为 V1。

2. 组网图

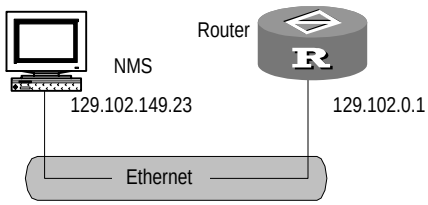

图8-2 SNMP 配置举例组网图

3. 配置步骤

第一步：设置团体名和访问权限

```
[Quidway] snmp-agent community read public
```

```
[Quidway] snmp-agent community write private
```

第二步：设置管理员标识、联系方法以及路由器物理位置

```
[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor
```

第三步：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
[Quidway] snmp-agent target-host trap address udp-domain 129.102.149.23
udp-port 5000 params securityname public
```

4. 配置 NMS

以 IBM 的 xnmbrowser 为例，设置 Name of IP Address 为 129.102.0.1，Community Name 为 **private**。现在就可以用 NMS 的客户端程序对路由器进行查询和设置操作了。

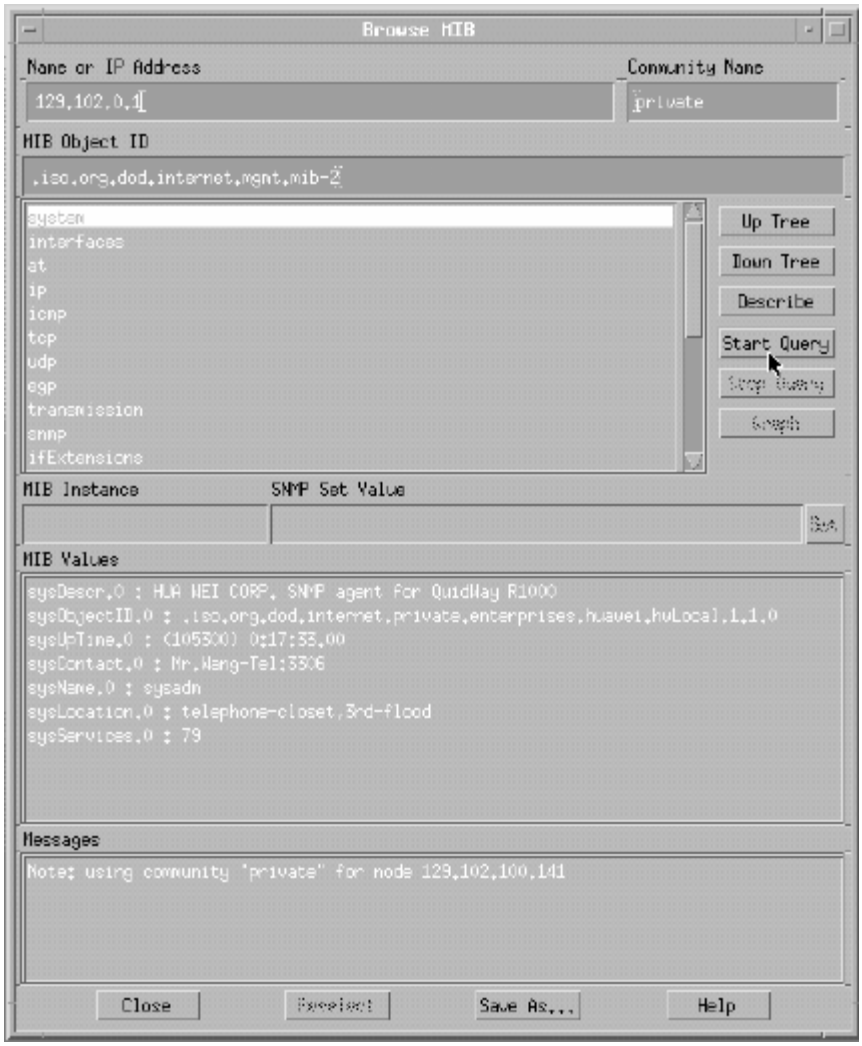

图8-3 NMS 用户界面

如上图所示，输入要查询的实例 iso.org.dod.internet.mgnt.mib-2.system，用单击按钮<Start Query>则会得到以下结果：

```
SysDescr.0 ： STRING: HUA WEI CORP. SNMP agent for QuidWay Routers
SysUpTime.0 ：(105300) 00:17:33:00
SysContact.0 ：    Mr.Wang-Tel:3306
SysName.0 ：       sysadm
SysLocation.0 ：   telephone-closet,3rd-floor
SysServices.0 ：   79
```

如果对 MIB 中的管理变量的含义不理解可用单击按钮<Describe>即可得到相应解释。

第9章 BIMS 配置

9.1 BIMS 概述

当通过 SNMP、Telnet 等方式管理网络设备时，一般需要知道设备 IP 地址等信息，这对于通过 DHCP 方式获得地址或 NAT 后面的设备，增加了主动管理的难度。BIMS（Branch Intelligent Management System）就是要解决上述问题，实现设备自动更新配置文件和应用程序功能。

BIMS 分 BIMS 中心侧和 BIMS 设备侧两个部分，其基本原理是：设备侧启动中或启动以后按照某种策略定期或间隔一定的时间向 BIMS 中心发出特定的信息请求，BIMS 中心侧根据管理员下达的策略指示同设备进行信息交互。在中心侧和设备侧的信息交互过程中，管理员可以对设备进行管理，执行诸如升级软件版本、更改配置、查看配置信息和状态信息等任务，从而达到管理员对设备实施集中管理的功能。

BIMS 中心侧可以是运行于 PC 或服务器上的服务软件（例如华为公司的 Quidview 网管系统 V3.10 的 BIMS 业务组件），BIMS 设备侧部分则集成在设备的软件系统中，实现 BIMS 功能的设备通过访问 BIMS 中心侧的服务器或 PC 来实现设备自动更新配置文件和应用程序。

BIMS 特性主要实现了以下功能：

- 支持通过执行命令立即访问 BIMS 中心获取新的配置文件或应用程序；
- 支持在设备启动时立即访问 BIMS 中心获取新的配置文件或应用程序；
- 支持设备每隔一定间隔时间访问 BIMS 中心获取新的配置文件或应用程序；
- 支持设备在某一特定时间点访问 BIMS 中心获取新的配置文件或应用程序。

设备使用 BIMS 功能进行配置文件或应用程序更新的过程如下：

- 在访问 BIMS 中心侧之前，设备必须开启 BIMS 功能，预先配置好设备的唯一标识符，BIMS 中心的 IP 地址，设备和 BIMS 中心双方的共享密钥。
- 设备因为某种原因被触发后，发送请求消息给 BIMS 中心，请求 BIMS 中心检查设备上的文件是否需要更新。
- BIMS 中心根据请求消息中上传的设备文件信息，判断各文件是否需要更新，需要更新则在回应消息中携带配置更新文件或需要更新的设备软件的 URL 路径信息和特征信息，或者是在回应消息中携带需要设备执行的命令内容及参数。
- 设备解析 BIMS 的回应消息，得到要更新的设备软件的 URL 或设备的加密后的配置文件或是需要执行的命令及参数。

- 设备得到配置文件后，执行配置文件命令并保存。
- 设备通过得到的 URL 向 BIMS 中心请求下载设备文件。
- 设备对从中心侧得到的设备软件校验后更新，之后给 BIMS 中心发确认消息。
- BIMS 中心侧根据设备发送的确认消息内容记录日志，并对设备发送的确认消息进行回应。

9.2 BIMS 配置

BIMS 为用户提供了一个很方便的管理方式，对设备提供了一个智能性的配置文件和应用程序的更新功能。对于设备侧来说主要包括以下几个方面的配置，其中启动 BIMS 功能、配置设备的唯一标识符、配置 BIMS 中心的 IP 地址和端口以及 BIMS 双方的共享密钥是必须配置的，而设备访问 BIMS 中心的方式则可以选择配置，既可以是上电时自动访问后按照一定间隔时间进行访问，也可以是在指定的时间段内按照一定的时间间隔访问，或者是执行命令使设备立即访问 BIMS 中心：

- 配置是否启动 BIMS 功能
- 配置设备的唯一标识符
- 配置 BIMS 中心的 IP 地址和端口号
- 配置 BIMS 设备发送报文时携带的源 IP 地址
- 设置 BIMS 设备侧和 BIMS 中心侧的共享密钥
- 配置当设备上电时是否触发设备访问 BIMS 中心
- 配置触发访问 BIMS 中心的间隔时间
- 配置设备在某一特定的时间访问 BIMS 中心以及访问的周期
- 配置设备立即访问 BIMS 中心。

9.2.1 配置是否启动 BIMS 功能

在设备上配置是否启动 BIMS 功能。

请在系统视图下进行下列配置。

表9-1 配置是否启动 BIMS 功能

操作	命令
配置在设备上启动 BIMS 功能	**bims enable**
取消在设备上启动 BIMS 功能	**undo bims enable**

9.2.2 配置设备唯一标识符

配置设备的唯一标识符，BIMS 中心根据设备的唯一标识符区分不同的设备。

请在系统视图下进行下列配置。

表9-2 配置设备的唯一标识符

操作	命令
配置设备的唯一标识符	**bims device-id** *string*
删除设备的唯一标识符	**undo bims device-id**

标识符最大长度 30 个字符。缺省情况下，没有配置设备的唯一标识符。

9.2.3 配置 BIMS 中心的 IP 地址和端口号

配置 BIMS 中心的 IP 地址和使用的端口号。

请在系统视图下进行下列配置。

表9-3 配置 BIMS 中心的 IP 地址和使用的端口号

操作	命令
配置 BIMS 中心的 IP 地址和使用的端口号	**bims ip address** *ip-address* [**port** *portnumber*]
删除配置的 BIMS 中心的 IP 地址	**undo bims ip address**

在配置 BIMS 中心的 IP 地址时，不输入端口号则默认为 BIMS 中心使用的端口号为 80。

缺省情况下，没有配置 BIMS 中心的 IP 地址。

9.2.4 配置 BIMS 设备发送报文时携带的源 IP 地址

可以使用某个接口的 IP 地址作为 BIMS 设备发送报文时携带的源 IP 地址。

请在系统视图下进行下列配置。

表9-4 配置 BIMS 设备发送报文时携带的源 IP 地址

操作	命令
配置 BIMS 设备发送报文时携带的源 IP 地址	**bims source ip-address** *ip-address*
删除配置的源 IP 地址	**undo bims source ip-address**

缺省情况下，BIMS 设备未配置源 IP 地址。

9.2.5 配置 BIMS 设备侧和中心侧的共享密钥

设置 BIMS 设备侧和 BIMS 中心侧的共享密钥。

请在系统视图下进行下列配置。

表9-5 配置 BIMS 设备侧和 BIMS 中心侧的共享密钥

操作	命令
设置 BIMS 设备侧和 BIMS 中心侧的共享密钥	**bims sharekey** { **simple** | **cipher** } *sharekey*
删除 BIMS 设备侧和 BIMS 中心侧之间的共享密钥	**undo bims sharekey**

共享密钥的长度为 16 位，缺省情况下，没有共享密钥。

9.2.6 配置当设备上电时是否触发设备访问 BIMS 中心

当配置了在设备上电时触发访问 BIMS 中心，则在设备上电启动完成后，立即访问 BIMS 中心。

请在系统视图下进行下列配置。

表9-6 配置当设备上电时是否触发设备访问 BIMS 中心

操作	命令
配置设备上电时访问 BIMS 中心	**bims boot request**
配置设备上电时不需要立即访问 BIMS 中心	**undo bims boot request**

缺省情况下，设备上电时不需要立即访问 BIMS 中心。

9.2.7 配置触发访问 BIMS 中心的间隔时间

配置了触发访问 BIMS 中心的间隔时间后，设备按照该时间间隔周期性地访问 BIMS 中心。

请在系统视图下进行下列配置。

表9-7 配置触发访问 BIMS 中心的间隔时间

操作	命令
配置触发访问 BIMS 中心的间隔时间	**bims interval** *number*
取消配置的访问 BIMS 中心的间隔时间	**undo bims interval**

number 为 0 表示不触发访问 BIMS 中心，取值范围为 0~9999，单位为小时。缺省情况下，没有配置该时间间隔。

9.2.8 配置设备在某一特定的时间访问 BIMS 中心以及访问的周期

配置设备在某一特定的时间访问 BIMS 中心，并在此基础上设定特定的访问周期以及访问的截止时间。

请在系统视图下进行下列配置。

表9-8 配置设备在某一特定的时间访问 BIMS 中心以及访问的周期

操作	命令
配置设备在特定的时间点访问 BIMS 中心，以及访问的周期和截至时间	**bims specify-time** *hh:mm yyyy/mm/dd* [[*hh:mm yyyy/mm/dd*] **period** *numberdays*]
取消该配置	**undo bims specify-time**

9.2.9 配置设备立即访问 BIMS 中心

执行该命令则设备立即访问一次 BIMS 中心。

请在系统视图下进行下列配置。

表9-9 配置设备立即访问一次 BIMS 中心

操作	命令
配置设备立即访问一次 BIMS 中心	**bims request**

9.3 BIMS 配置调试

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

在用户视图下，执行 **debugging** 命令可以打开调试开关或者显示其各项状态参数，从而可以监控和维护 BIMS 配置。

表9-10 BIMS 配置的调试

操作	命令
打开 BIMS 调试信息开关	**debugging bims all**
关闭 BIMS 调试信息开关	**undo debugging bims all**

9.4 BIMS 典型配置举例

9.4.1 配置设备上电后立即访问 BIMS 中心

1. 组网需求

设备上电后立即访问 BIMS 中心（IP 地址为 10.153.21.97，使用的端口号为 80），并且以后每隔 48 个小时访问一次 BIMS 中心。

2. 配置步骤

- BIMS 中心的配置

BIMS 中心一般采用华为 3Com 公司的 Quidview 网管系统的 BIMS 组件，在该组件中，需要作如下设置：

(1) 在“参数设置”界面中设置 BIMS 中心侧和设备侧的共享密钥，该共享密钥必须与设备侧设置的一致。

(2) 将设备添加到网管系统中进行管理：设备可以通过两种方式增加到网管系统中：

手工增加：用户输入设备的名称，在系统中添加该设备。

当设备访问 BIMS 中心时自动增加：采用自动增加方式时需要预先打开“自动添加上报设备”的开关，同时设置好 BIMS 中心侧与设备侧公用的密钥，这样当设备访问 BIMS 中心时，如果该设备还没有添加到 BIMS 中心，系统会自动添加该设备。

(3) 为设备指定待升级的文件：包括配置文件以及应用软件，当设备访问 BIMS 中心时，系统会进行判断，确定是否要用待升级的文件升级设备上的文件。如果需要更新，则 BIMS 中心会将待升级文件下发到设备上，升级设备上相应的文件。

📖 说明：

关于华为 3Com 公司的 Quidview 网管系统 BIMS 组件的详细使用说明，请参见 Quidview 网管系统 BIMS 组件的用户手册。

- 设备侧的配置

进入系统视图。

```
<Quidway> system-view
```

#在设备上配置启动 BIMS 功能。

```
[Quidway] bims enable
  bims is enable
```

#配置设备的唯一标识符为 ar18-20-907。

```
[Quidway] bims device-id ar18-20-907
```

#配置 BIMS 设备侧和中心侧的共享密钥。

```
[Quidway] bims sharekey simple 1122334455667788
```

#配置 BIMS 中心的 IP 地址，使用缺省的端口号 80。

```
[Quidway] bims ip address 10.153.21.97
```

#配置设备上电后立即访问 BIMS 中心。

```
[Quidway] bims boot request
```

#配置触发访问 BIMS 中心侧的间隔时间。

```
[Quidway] bims interval 48
```

进行上述配置后，设备在上电后立即访问 BIMS 中心，并且以后每隔 48 个小时访问一次 BIMS 中心。在设备每次访问 BIMS 中心时，BIMS 中心都会根据该设备的待升级文件列表来判断是否需要用待升级文件更新设备的相应文件。如果需要，则执行下发文件操作，更新设备侧的相应文件。

9.4.2 配置设备在一定时间段内周期性访问 BIMS 中心

1. 组网需求

设备从 2005 年 5 月 1 日 12 点 10 分开始访问 BIMS 中心（IP 地址为 10.153.21.97，使用的端口号为 80），每隔 2 天访问一次，直到 2005 年 10 月 1 日 23 点 50 分截至。

2. 配置步骤

BIMS 中心的配置请参见上面的例子。下面只描述设备侧的相关配置步骤。

进入系统视图。

```
<Quidway> system-view
```

#在设备上配置启动 BIMS 功能。

```
[Quidway] bims enable
  bims is enable
```

#配置设备的唯一标识符为 ar18-20-907。

```
[Quidway] bims device-id ar18-20-907
```

#配置 BIMS 设备侧和中心侧的共享密钥。

```
[Quidway] bims sharekey simple 1122334455667788
```

#配置 BIMS 中心的 IP 地址，使用缺省的端口号 80。

```
[Quidway] bims ip address 10.153.21.97
```

#配置设备从 2005 年 5 月 1 日 12 点 10 分开始访问 BIMS 中心，每隔 2 天访问一次，直到 2005 年 10 月 1 日 23 点 50 分截至。

```
[Quidway] bims specify-time 12:10 2005/05/01 23:50 2005/10/01 period 2
```

进行上述配置后，设备在指定的时间段内按照指定的访问时间间隔对 BIMS 中心进行访问。在设备每次访问 BIMS 中心时，BIMS 中心都会根据该设备的待升级文件列表来判断是否需要用待升级文件更新设备的相应文件。如果需要，则执行下发文件操作，更新设备侧的相应文件。

第10章 RMON 配置

10.1 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 MIB 由一组统计数据、分析数据和诊断数据组成。不像标准 MIB 仅提供被管理对象大量的关于端口的原始数据，它提供的是一个网段的统计数据和计算结果。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，跟踪统计其接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。

目前 VRP 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，NMS 可以获得与被管理网络设备接口相连的网段上的整体流量、错误统计和性能统计等信息，从而实现对网络的管理。

10.2 RMON 的配置

📖 说明：

在配置 RMON 功能之前，应先配置 SNMP agent，保证 NMS 可以管理路由器，这样用户才能通过 NMS 查询告警、日志等信息。

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/删除历史控制表的一个表项
- 添加/删除 RMON 告警扩展表的一个表项
- 添加/删除统计表的一个表项

10.2.1 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10-1 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*

10.2.2 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（如接口的统计数据）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10-2 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** *alarm-entry 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** *alarm-entry*

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按照定义的时间间隔进行采样

(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10-3 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	触发所定义的事件
采样值小于等于设定的下限	触发所定义的事件

10.2.3 添加/删除 RMON 告警扩展表的一个表项

该命令用来在 RMON 告警扩展表中添加/删除一个表项。告警扩展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：

在添加告警扩展表项之前，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10-4 在 RMON 告警扩展表中添加/删除一个表项

操作	命令
在 RMON 告警扩展表中添加一个表项	**rmon prialarm** *prialarm-entry 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 RMON 告警扩展表中删除一一个表项	**undo rmon prialarm** *entry-number*

用户定义了告警扩展表项后，系统对告警表项的处理如下：

(1) 对所定义的告警变量按照定义的时间间隔进行采样

(2) 将采样值按照定义的运算公式进行计算

(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10-5 告警扩展表项的处理过程

实际情况	处理过程
计算值大于等于设定的上限	触发所定义的事件
计算值小于等于设定的下限	触发所定义的事件

10.2.4 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接口的数据。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。

请在以太网接口视图进行下列配置。

表10-6 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个表项	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text-string*]
在历史控制表中删除一个表项	**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。

10.2.5 添加/删除统计表的一个表项

利用 RMON 统计管理功能，可以监视接口的使用情况、统计接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。

请在以太网接口视图下进行下列配置。

表10-7 在统计表中添加/删除一个表项

操作	命令
在统计表中添加一个表项	**rmon statistics** *entry-number* [**owner** *text-string*]
在统计表中删除一个表项	**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。

10.2.6 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 RMON 的统计表、历史控制表、告警表、告警扩展表、事件表、事件日志中的信息。

表10-8 RMON 显示和调试

操作	命令
显示 RMON 统计表	**display rmon statistics** [*interface-type interface-number*]
显示 RMON 历史控制表	**display rmon history** [*interface-type interface-number*]
显示 RMON 告警表	**display rmon alarm** [*alarm-entry*]
显示 RMON 告警扩展表	**display rmon prialarm** [*prialarm-entry*]
显示 RMON 事件表	**display rmon event** [*event-entry*]
显示 RMON 事件日志	**display rmon eventlog** [*event-entry*]

10.3 RMON 典型配置举例

1. 组网需求

被检测路由器 RouterA 通过 console 口连接配置终端，通过以太网连接 NMS。NMS 使用 Quidview 网管系统，可以通过网管查询路由器的运行状况。

配置需求：

- 在 RMON 告警表中设定一个表项，1.3.6.1.2.1.16.1.1.1.4.1 节点的相对采样值超过上下限阈值分别可以触发两个 trap 事件；
- 进行以太网接口性能统计；
- 通过 **display rmon statistics** 命令查看显示结果，同时在网管上查看统计结果。

2. 组网图

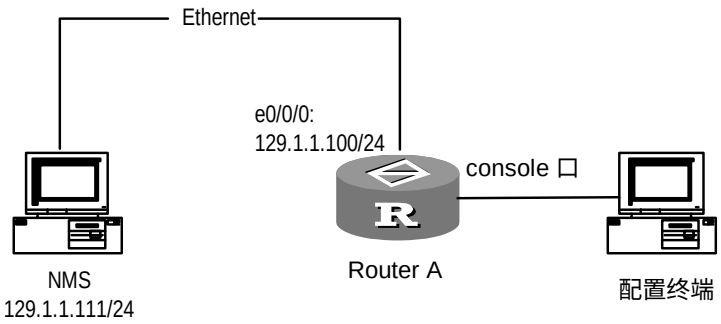

图10-1 RMON 典型应用举例

3. 配置步骤

配置 SNMP（注意：SNMP 的读、写团体及版本应与 Quidview 侧的配置一致）。

```
[Quidway] snmp-agent
[Quidway] snmp-agent community read public
[Quidway] snmp-agent community write private
[Quidway] snmp-agent sys-info version v1
[Quidway] snmp-agent trap enable
[Quidway] snmp-agent target-host trap address udp-domain 129.1.1.111 params
securityname huawei
```

配置 RMON 告警表项。

```
[Quidway] rmon event 1 description rising trap router1 owner huawei-rmon
[Quidway] rmon event 1 description falling trap router1 owner huawei-rmon
[Quidway] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising_threshold 100
1 falling_threshold 50 2
```

配置以太网口 IP 地址。

```
[Quidway] interface ethernet 0/0/0
[Quidway-Ethernet0/0/0] ip address 129.1.1.100 255.255.255.0
```

配置 RMON 对以太网口进行统计。

```
[Quidway-Ethernet0/0/0] rmon statistics 1 owner huawei-rmon
[Quidway-Ethernet0/0/0] quit
```

查看 RMON 告警表信息及以太网口的统计信息。

```
<Quidway> display rmon alarm 1
<Quidway> display rmon statistics ethernet 0/0/0
```

当告警事件被触发时在 Quidview 的告警管理部分可以查看相应的记录。

第11章 终端服务

11.1 终端服务简介

系统提供多种终端服务，使用户可以进入命令行接口：

- 通过 Console 口进行本地配置
- 通过 AUX 口进行远程或本地配置
- 通过 Telnet 或者 SSH 进行本地或远程配置
- PAD 终端服务
- 哑终端服务

11.2 Console 口终端服务

通过 Console 口即控制台，可以建立本地配置环境。配置环境的搭建参见第 1 章相关内容。

Console 口终端服务特性参见下表。

表11-1 Console 口终端服务特性

服务	特性
回显方式	本地不回显
终端类型	VT100
波特率	9600
数据位	8
奇偶校验	无
停止位	1 位
流控	无
二进制传输协议	XModem

11.3 AUX 口的远程终端服务

11.3.1 功能描述

AUX 口除了可以如 CON 口一样进行本地配置外，还可以进行远程配置，本地配置的方法请参见上一节，本节主要讲述远程终端服务。

系统支持通过 AUX 口对路由器进行远程配置，在微机串口和路由器 AUX 口上挂接 Modem，通过 PSTN 相连，在微机上通过拨号建立与远端路由器的连接。拨号成功后，用户可以从终端敲入配置命令，设置远端路由器工作参数。

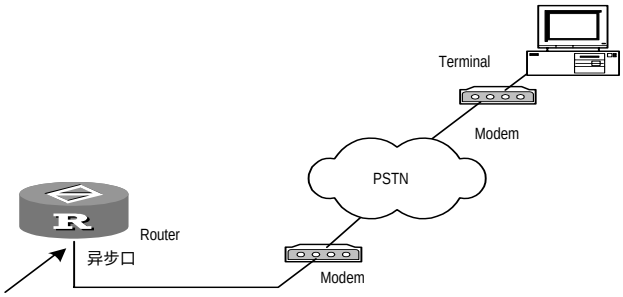

图11-1 通过异步口搭建远程配置环境

11.3.2 AUX 口的远程配置终端服务特性

系统的远程配置终端服务特性参见下表。

表11-2 远程终端服务特性

服务	特性
回显方式	本地不回显
终端类型	VT100
波特率	与接口配置一致，缺省为 9600bps
数据位	与接口配置一致，缺省为 8 位
奇偶校验	与接口配置一致，缺省无
停止位	与接口配置一致，缺省为 1 位
流控	与接口配置一致，缺省无

在微机上运行的终端程序需按上表设置参数，其中波特率、数据位、奇偶校验及流控等参数要与相应的路由器 AUX 口的配置一致。

11.4 Telnet 终端服务

11.4.1 Telnet 服务种类

Telnet 协议在 TCP/IP 协议族中属于应用层协议，通过网络提供远程登录和虚拟终端功能。路由器系统提供的 Telnet 服务包括：

1. Telnet Server 服务

如下图所示，用户在微机上可以运行 Telnet 客户端程序登录到路由器上，对路由器进行配置管理。

图11-2 提供 Telnet Server 服务

2. Telnet Client 服务

如下图所示，用户在微机上通过终端仿真程序或 Telnet 程序建立与路由器的连接后，可以输入 Telnet 命令再登录其它路由器，对其进行配置管理。

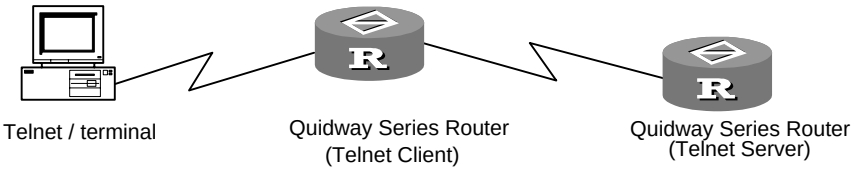

图11-3 提供 Telnet Client 服务

路由器系统的 Telnet 服务特性参见下表。

表11-3 Telnet 服务特性

服务	特性
输入模式	字符模式
回显方式	本地不回显
终端类型	VT100

3. 重定向终端服务

利用重定向终端服务功能，当用户通过 Telnet 客户端程序以特定的端口号登录路由器时，可以实现重定向连接，登录到与路由器异步口（即 TTY 接口）相连的设备上。典型的应用是将路由器的 8/16 异步口以直连方式外接多个设备，实现对这些设备的远程配置和维护。

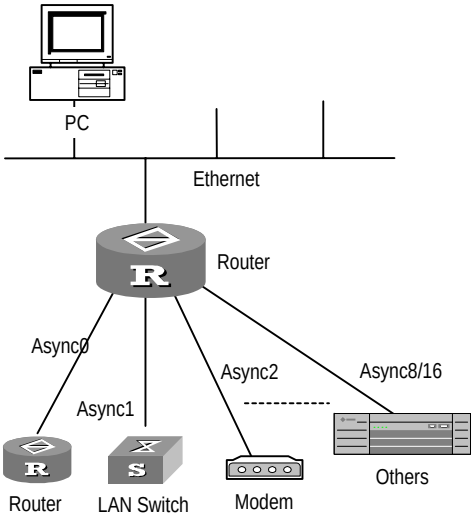

图11-4 提供 Telnet 重定向服务

11.4.2 建立 Telnet 连接

1. 建立 Telnet 连接

请在用户视图下进行下面配置。

表11-4 建立 Telnet 连接

操作	命令
执行 Telnet 命令登录并管理其它路由器	**telnet** [**vpn-instance** *vpn-instance-name*] *host-ip-address* [*service-port*]

例：PC 通过 Console 口与路由器 Quidway1 建立连接，再执行 Telnet 命令登录路由器 Quidway2，其 IP 地址为 129.102.0.1。

```
<Quidway1> telnet 129.102.0.1
Trying  129.102.0.1 ...
Connected to 129.102.0.1 ...
<Quidway2>
```

2. 配置 Telnet 超时时间

请在用户界面视图下进行下面配置。

表11-5 配置 Telnet 超时时间

操作	命令
允许定时断开 Telnet 连接	**idle-timeout** *minutes* [*seconds*]
恢复定时断连缺省设置	**undo idle-timeout**

缺省情况下，超时时间为 10 分钟。

3. 配置 Telnet 源接口/源地址

请在用户视图下进行下面配置。

表11-6 配置 Telnet 源接口/源地址

操作	命令
在指定接口的主 IP 地址和目的地址之间建立 Telnet 连接	**telnet** *ip-address* [*port*] **source-interface** *interface-type interface-number*
在指定的源 IP 地址和目的地址之间建立 Telnet 连接。	**telnet** *ip-address* [*port*] **source-ip** *source-address*

当同时配置了源接口和源 IP 地址时，后者有效。

该命令一般配合 ACL 使用。例如，当在 Telnet Client 端指定一个 loopback 接口为源接口时，其 Telnet 连接的源 IP 就是该接口的主 IP 地址，这样在 Telnet Server 端配置 ACL 时只需针对一个 IP 地址配置访问控制策略即可。

11.4.3 建立 Telnet 重定向连接

为了实现重定向连接，事先需要对路由器做好如下配置：

- 将异步接口配置为“流”方式（**flow**）；
- 启动重定向功能（**redirect**）；
- 禁止在用户界面上启动终端服务。
- 配置用户界面相关选项
- 断开 Telnet 重定向连接

1. 配置异步接口

表11-7 配置异步接口为流模式

操作	命令
配置外接设备的路由器异步口为流方式（异步接口视图）	**async mode flow**
打开或禁止 **dsr-dtr** 检测（异步接口视图）	**detect dsr-dtr** **undo detect dsr-dtr**
配置 tty 接口不采用流控（tty 类型的用户界面视图）	**flow-control none**

异步接口缺省的模式为 **protocol** 模式，允许 **dsr-dtr** 检测，不进行流控。

注意：Quidway 系列路由器的异步接口为 7 线制，缺省为允许 **dsr-dtr** 检测；但若对端设备为 3 线制时（如 NE 路由器），不可能发送 **dsr-dtr** 信号，故此时应在 Quidway 系列路由器上配置 **undo detect dsr-dtr** 命令，以保证串口能够在不检测 **dsr-dtr** 信号的条件下 UP。

2. 启动 Telnet 重定向功能

在接口视图下执行 **undo shell** 命令。

请在用户界面视图下执行 **redirect enable** 命令，使能端口重定向功能。

表11-8 建立 Telnet 重定向连接

操作	命令
使能 Telnet 重定向功能（只对 AUX、TTY 类型接口有效）	**redirect enable**
禁止在用户界面上启动终端服务，允许该接口启动 telnet 重定向。	**undo shell**

3. 配置监听端口

请在用户界面视图下进行下面配置。

表11-9 配置用户界面的相关选项

操作	命令
设置 telnet 重定向的监听端口	**redirect listen-port** *port-number*
恢复缺省的监听端口	**undo redirect listen-port** *port-number*

缺省的监听端口为 TTY 序号加 2000。

4. 配置用户界面其他相关参数

请在用户界面视图下进行下面配置。

表11-10 配置用户界面的相关选项

操作	命令
设置 telnet 重定向的空闲超时时间	**redirect timeout** *minutes*
设置 telnet 重定向连接永远不超时	**undo redirect timeout**
设置 telnet 重定向路由器对从 telnet 客户端接收到的回车符进行处理	**redirect return-deal from-telnet**
设置 telnet 重定向路由器不对回车符进行处理	**undo redirect return-deal from-telnet**
设置 telnet 重定向路由器对从终端接收到的回车符进行处理	**redirect return-deal from-terminal**
设置 telnet 重定向路由器不对回车符进行处理	**undo redirect return-deal from-terminal**
设置在建立 telnet 重定向连接时进行 telnet 选项协商	**redirect refuse-negotiation**
设置在建立 telnet 连接时不进行选项协商。	**undo redirect refuse-negotiation**

缺省的超时时间为 360 秒，回车符不处理，进行 telnet 选项协商。

5. 断开 Telnet 重定向连接

请在用户界面视图下进行下面配置。

表11-11 断开 Telnet 重定向连接

操作	命令
断开已经建立的 telnet 重定向连接	**redirect disconnect**

使用组合键<Ctrl+]>，终止重定向连接。

📖 说明：

与路由器异步接口相连的设备接口也必须工作在异步流方式下。

建立重定向连接时的 Telnet 端口号按如下规则编号：Telnet 端口号等于 TTY 编号加上 2000。可以使用 display user-interface 命令，显示出各用户界面及其编号。其中 TTY 用户界面编号是与路由器各异步接口一一对应的。TTY 编号规则请参见 3.1.2 用户界面的编号。

与路由器的第七个异步串口相连的外接设备为 D，现通过 Telnet 与 D 通信。路由器的 IP 地址为 10.110.164.44。（假设路由器及外接设备相关配置已经配置好。）

```
<Quidway> telnet 10.110.164.44 2007
Trying  10.110.164.44 ...
Connected to 10.110.164.44
```

Telnet 重定向连接建立成功后，可以发送命令与异步口连接设备通信。如果连接的是 Modem 设备，则可以通过 AT 命令探测 Modem 状态或配置 Modem。例：

at

OK

键入快捷键<Ctrl+]>，将终止 Telnet 重定向连接。

11.4.4 Telnet 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 Telnet 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 Telnet 进行调试。

表11-12 Telnet 连接的显示和调试

操作	命令
显示当前用户界面连接情况	**display users**
显示每个用户界面连接情况	**display users all**
显示当前建立的所有 TCP 连接情况	**display tcp status**

操作	命令
打开 Telnet 连接的调试开关	**debugging telnet**
关闭 Telnet 连接的调试开关	**undo debugging telnet**

display users 命令只能显示与路由器连接的 Telnet 客户使用的接口。如果要查看与路由器建立连接的 Telnet 服务器 IP 地址，则需要执行 **display tcp status** 命令，其中端口号为 23 的 TCP 连接均为 Telnet 连接，包括 Telnet 客户和 Telnet 服务器连接。

在 Telnet 连接过程中，可以使用快捷键来中断连接。如下图所示，终端运行 Telnet 客户端程序登录到 RTA，然后，再 Telnet 连接到 RTB，再 Telnet 连接到 RTC，成为级连结构，此时，RTA 是 RTB 的 client，RTB 是 RTC 的 client，下面，以此结构简单地说明快捷键的用法：

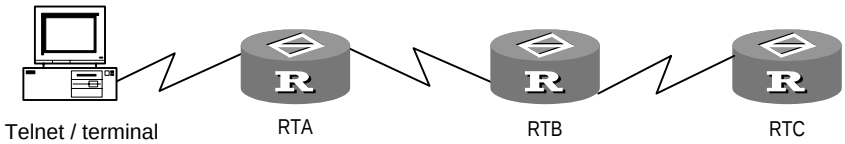

图11-5 Telnet 快捷键使用示意图

1. <Ctrl+]>快捷键

在网络畅通的情况下，键入<Ctrl+]>，就是通知 Telnet 服务器端要中断本次 Telnet 登录，作用与 **Quit** 命令一样，即服务器端主动断开连接；如果由于某些原因网络断了，则快捷键的指令不能传送到服务器端，输入无效。

<RTC> （此时键入<Ctrl+]>，将退回到 RTB 的提示符。）

<RTB> （此时键入<Ctrl+]>，将退回到 RTA 的提示符。）

<RTA> （此时键入<Ctrl+]>，将退出 Telnet 连接。）

2. <Ctrl+k>快捷键

在服务器端故障且客户端无法感知的情况下，此时，客户端输入任何指令服务器均无响应，这种情况下，键入<Ctrl+k>快捷键，客户端主动中断本次连接，并直接退出 Telnet 连接。

<RTC> （此时键入<Ctrl+k>，将直接中断，并退出 Telnet 连接。）

11.4.5 Telnet 重定向典型配置举例 1

1. 组网需求

PC 的地址为 201.1.1.2，路由器 A 的 Ethernet0/0/0 地址为 201.1.1.1，同时路由器的 async1/0/0 和路由器 B 的 console 接口相连，同时确定对应关系为 async1/0/0 对应的 tty 为 user-interface tty 1。

2. 组网图

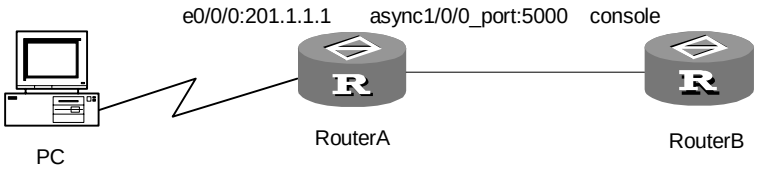

图11-6 Telnet 重定向典型配置举例

3. 配置步骤

配置 RouterA：

配置 Ethernet0/0/0。

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
```

配置 async1/0/0。

```
[Router] interface async1/0/0
[Router-async0/0/0] async mode flow
[Router-async0/0/0] flow-control none
```

启动 Telnet 重定向，并配置用户界面相关参数。

```
[Router] user-interface tty 1
[Router -ui-tty1] undo shell
[Router -ui-tty1] redirect enable
[Router -ui-tty1] undo redirect timeout
[Router -ui-tty1] redirect listen-port 5000
[Router -ui-tty1] redirect refuse-negotiation
```

通过上面的配置可以在 PC 上使用 telnet 201.1.1.1 5000 建立 telnet 客户界面对 RouterB 进行控制管理。而且连接永远不会超时，同时不进行 telnet 选项协商。对于该配置，PC（telnet 客户端）的所有数据将被透明的传输到 RouterB，同时 RouterB 的所有数据将透明的传输到 PC（telnet 客户端）。

这时候，如果 telnet 客户端在输入回车时会发送“ 0x0d 0x0a ”，这样可能造成在输入一个回车时，客户端回显示两条冗余信息，对于这个问题可以在 user-interface tty 1 增加下面的配置即可解决。

```
[Router -ui-tty1] redirect return-deal from-telnet
```

11.4.6 Telnet 重定向典型配置举例 2

1. 组网需求

假设路由器 A 的 Ethernet0/0/0 地址为 201.1.1.1，PC 的地址为 201.1.1.2，同时路由器 A 的 async1/0/0 和路由器 B 的 console 接口相连，同时确定 async1/0/0 对应的 tty 为 user-interface tty 1。同时路由器 A 的 async1/1/0 和另外一台路由器 C 的 console 接口相连，同时确定 async1/1/0 对应的 tty 为 user-interface tty 2。

2. 组网图

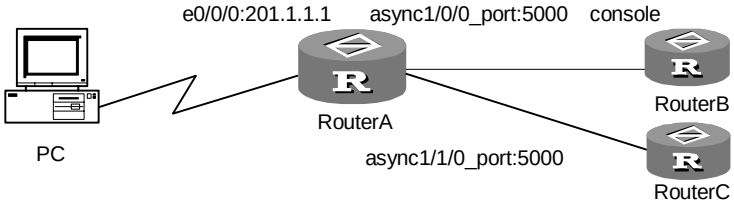

图11-7 Telnet 重定向典型配置举例

3. 配置步骤

配置 Ethernet0/0/0。

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
```

配置 async1/0/0 及 async1/1/0。

```
[Router] interface async1/0/0
[Router-async1/0/0] async mode flow
[Router-async1/0/0] flow-control none
[Router-async1/0/0] interface async1/1/0
[Router-async1/1/0] async mode flow
[Router-async1/1/0] flow-control none
```

#启动 Telnet 重定向，并配置用户界面相关参数。

```
[Router] user-interface tty 1 2
[Router -ui-tty1-2] undo shell
[Router -ui-tty1-2] redirect enable
[Router -ui-tty1-2] undo redirect timeout
[Router -ui-tty1-2] redirect listen-port 5000
[Router -ui-tty1-2] redirect refuse-negotiation
[Router -ui-tty1-2] redirect return-deal from-telnet
```

通过上面的配置可以在 PC 上执行一次 telnet 201.1.1.1 5000，可以建立 telnet 重定向连接对 RouterB 进行控制管理；如果再执行一次 telnet 201.1.1.1 5000，就可以建立 telnet 重定向连接对 RouterC 进行控制管理。这种情况一般用于在一个设备提供了两个控制终端时，这样可以节约端口号，同时易于管理。

11.5 PAD 终端服务

用户终端有两种：分组终端和非分组终端。分组终端（如计算机或智能终端等）发送和接收的均是规格化的分组，可以按照 X.25 协议直接与分组交换网相连。而非分组终端（如字符型终端）产生的用户数据不是分组，而是一连串字符（字节）。非分组终端不能直接接入分组交换网，而要通过报文分组汇集器/拆卸器 PAD（Packet Assembler/Disassembler）才能接入到分组交换网。

PAD 的主要功能是在发送端将非分组终端产生的一连串字符组装成分组，以便送入分组交换网中传输；在接收端将接收到的分组拆卸成字符以便非分组终端接收。

VRP 支持 X.25 PAD 功能，X.25 PAD 是连接非 X.25 终端和 X.25 网络的桥梁，使得非 X.25 类型的终端可以通过其接入 X.25 网络。通过在不支持 X.25 规程的终端和 X.25 网络之间加入 PAD 设备，使非 X.25 终端可以通过 X.25 网络与其它终端进行通信。X.25 PAD 设备实际上是一个规程转换器或网络服务器，通过为各种不同的终端提供服务来帮助它们进入 X.25 网络。

关于 PAD 终端服务的详细介绍请参考本手册链路层协议中的‘ LAPB 和 X.25 配置 ”。

11.6 SSH 终端服务

11.6.1 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路由器时，SSH 特性可以提供安全保障和强大的认证功能，以保护路由器不受诸如 IP 地址欺诈、明文密码截取等等的攻击。路由器可以接受多个 SSH 客户的连接。SSH 客户端的功能是允许用户与支持 SSH Server 的路由器、UNIX 主机等建立 SSH 连接。如下图所示，可以通过本地连接或广域网连接建立 SSH 通道。

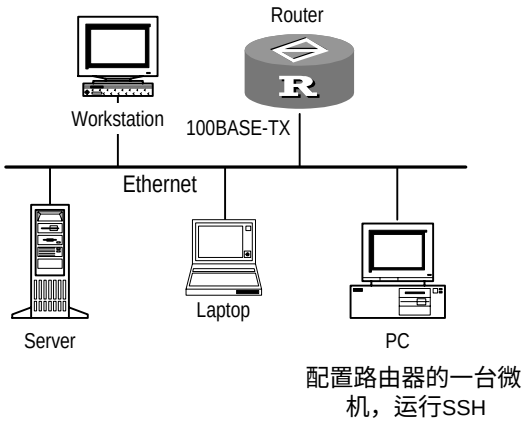

图11-8 在局域网内建立 SSH 通道

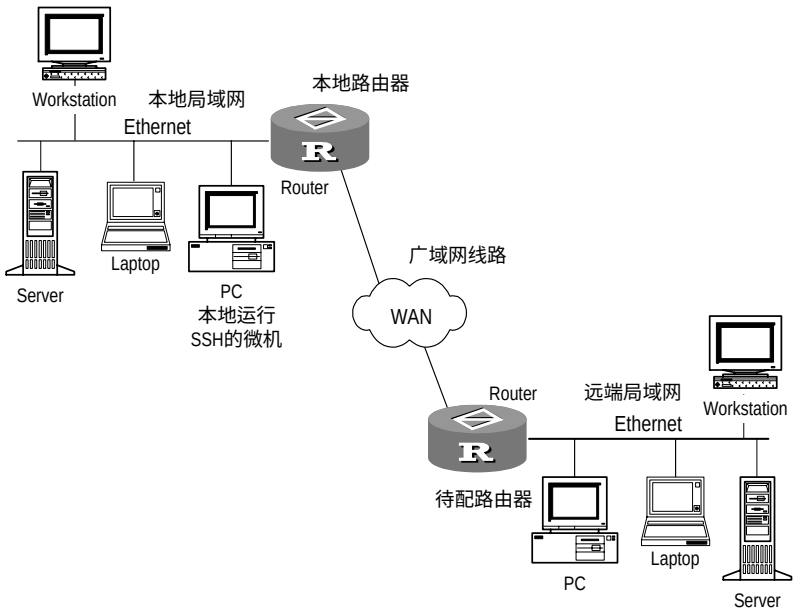

图11-9 通过广域网建立 SSH 通道

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、密钥算法协商阶段、认证方法协商阶段、会话请求阶段、交互会话阶段，完成实现 SSH 的认证安全连接。

11.6.2 SSH 配置

SSH 配置包括：

- 设置所在用户界面支持的协议
- 配置和销毁本地 RSA 密钥对
- 为 SSH 用户配置验证方式
- 设置服务器密钥的更新时间
- 设置 SSH 认证超时时间
- 设置 SSH 验证重试次数
- 进入公共密钥视图
- 进入公共密钥编辑视图，编辑密钥
- 退出公共密钥编辑视图，返回系统视图
- 为 SSH 用户分配公共密钥

11.6.3 设置所在用户界面支持的协议

该配置任务用来指定所在的用户界面支持的协议，缺省为支持 Telnet 和 SSH。如果使能 SSH 的情况下，本机 RSA 密钥没有配置，则仍然不能通过 SSH 登录。配置结果在下次登录请求时生效。

请在 VTY 类型的用户界面视图下进行下列配置。

表11-13 设置所在用户界面支持的协议

操作	命令
设置所在用户界面支持的协议	**protocol inbound** { **all** | **ssh** | **telnet** | **pad** }

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验证方式为 **authentication-mode scheme**；若配置其他验证方式为 **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。

1. 配置和销毁本地 RSA 密钥对

该配置任务用来产生本地服务器密钥对和主机密钥对，如果此时已经有了 RSA 密钥，系统提示是否替换原有密钥。产生的密钥对的命名方式分别为：路由器名称+server 和路由器名称+host。服务器密钥和主机密钥的位数相差至少 128 位，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11-14 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，一定记得完成 **rsa local-key-pair create** 配置，生成本地密钥对。此命令只需执行一遍，路由器重启后不必再次执行。

2. 为 SSH 用户配置验证方式

该配置任务用来为 SSH 用户指定验证方式。对于新的用户，必须指定验证方式，否则，无法登录。新建一个 SSH 用户的方法，请您参考本手册安全部分之“ AAA 及 RADIUS 配置 ”中的 **local-user** 命令的应用。新配置的验证方式在下次登录时生效。

请在系统视图下进行下列配置。

表11-15 为 SSH 用户配置验证方式

操作	命令
为 SSH 用户配置验证方式	**ssh user** *username* **authentication-type** { **password** | **RSA** | **all** }
恢复系统默认的无法登录方式	**undo ssh user** *username* **authentication-type**

📖 说明：

配置 password 认证时，*username* 应为 AAA 中定义的有效 SSH 用户名；配置 RSA 认证时，*username* 就是 SSH 本地用户名，与 AAA 中定义的用户无关。

3. 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，更大限度的保证您的 SSH 连接的安全性。

请在系统视图下进行下列配置。

表11-16 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**

系统缺省不对密钥进行更新。

4. 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11-17 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。

5. 设置 SSH 验证重试次数

该配置任务用来设置 SSH 用户请求连接的验证重试次数，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11-18 设置 SSH 验证重试次数

操作	命令
设置 SSH 验证重试次数	**ssh server authentication-retries** *times*
恢复 SSH 默认的验证重试次数	**undo ssh server authentication-retries**

系统默认的验证重试次数为 3。

6. 进入公共密钥视图

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。此时的客户端密钥，是由支持 SSH1.5 的客户端软件随机生成的。

请在系统视图下进行下列第一项配置。

表11-19 公共密钥配置

操作	命令
进入公共密钥视图	**rsa peer-public-key** *key-name*
从公共密钥视图退回到系统视图	**peer-public-key end**

7. 进入公共密钥编辑视图，编辑密钥

该配置任务用来进入公共密钥编辑视图，输入由客户端软件生成的公共密钥数据。在对公钥进行编辑前，一定要在系统视图下，使用 **rsa peer-public-key** *key-name* 命令指定一个密钥名称。

在输入密钥数据时，字符之间可以有空格，也可以按回车键继续输入数据，所配置的公钥必须是按公钥格式编码的十六进制字符串。

请在公共密钥视图下进行下列配置。

表11-20 编辑公共密钥

操作	命令
进入公共密钥编辑视图	**public-key-code begin**

8. 退出公共密钥编辑视图

该配置任务用来从公共密钥编辑视图退回到公共密钥视图，并保存输入的公钥数据，也用来从公共密钥视图退回到系统视图。

请在公共密钥编辑视图下进行下列配置。

表11-21 退出公钥编辑视图

操作	命令
退出公钥编辑视图	**public-key-code end**

9. 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11-22 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**

11.6.4 SSH 显示和调试

在完成上述配置后，在任何视图下执行 **display** 命令，可以显示配置后 SSH 的运行情况，通过查看显示信息，验证配置的效果。

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。

请在任何视图下进行下列 **display** 操作，在用户视图下执行下列 **debugging** 操作。

表11-23 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*]

表11-24 调测 SSH 相关信息

操作	命令
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** }

11.6.5 SSH 配置举例

1. 组网需求

配置终端（SSH Client）与路由器通过以太网口直接相连，在终端上运行 SSH1.5 的客户端软件可以安全地登录路由器进行配置管理。SSH Client 用户名为 client001@169.254.0.1，口令为 huawei。

2. 组网图

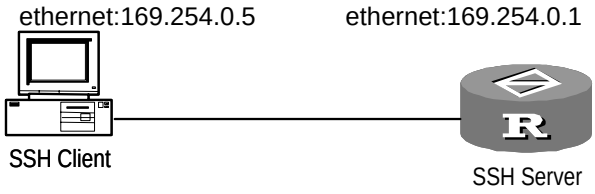

图11-10 SSH Server 配置组网图

3. 配置步骤

(1) 配置 SSH 服务器（路由器）

根据登录验证方式不同分别介绍配置步骤，但开始任何一种配置之前，首要执行如下操作：

```
[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。

- 配置 SSH 用户验证方式为 password。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode scheme
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
[Quidway] local-user client001
[Quidway-luser-client001] password simple huawei
[Quidway-luser-client001] service-type ssh
```

```
[Quidway-luser-client001] quit
[Quidway] ssh user client001 authentication-type password
[Quidway] domain 169.254.0.1
[Quidway-isp-169.254.0.1] scheme local
[Quidway-isp-169.254.0.1] quit
```

SSH 的验证超时时间、重试次数以及服务器密钥更新时间可以采用系统默认值，这些配置完成以后，您就可以在与路由器连接的其它终端上，运行支持 SSH2.0 的客户端软件，以用户名 client001，密码 huawei，访问路由器了。

- 配置 SSH 用户验证方式为 RSA。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode scheme
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
[Quidway] local-user client002
[Quidway-luser-client002] password simple huawei
[Quidway-luser-client002] quit
[Quidway] ssh user client002 authentication-type RSA
```

这时您需要在支持 SSH1.5 的客户端软件上，随机产生 RSA 密钥对（含公钥及私钥），并按如下方式将 RSA 公钥（此处的 RSA 公钥是指用我司提供的 SSHKEY.EXE 软件进行 PKCS 标准编码后的 16 进制字符串）配置到 SSH Server 上指定的 rsa peer-public-key 中。

```
[Quidway] rsa peer-public-key quidway002
[Quidway-rsa-public-key] public-key-code begin
[Quidway-rsa-key-code] 30818602818073 9A291ABDA704F5D93DC8FDF84C427463
[Quidway-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[Quidway-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[Quidway-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[Quidway-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[Quidway-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
[Quidway] ssh user client002 assign rsa-key quidway002
```

(2) 配置 SSH 客户端

- 对于 password 验证，需要在客户端上配置 SSH Server（路由器）可达接口的 IP 地址 169.254.0.1，协议类型为 SSH，版本为 1。打开 SSH 连接后按提示输入用户名及口令，即可进入路由器配置界面。

```
login as: client001
Sent username "client001"
client001@169.254.0.1's password:
```

```
*********************************************************
*          All rights reserved (1997-2004)              *
*      Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*********************************************************

<Router>
```

- 对于 RSA 验证，不仅需要在客户端上配置 SSH Server 的 IP 地址、协议类型、版本，还需要指定 RSA 私钥文件（由客户端软件随机产生的）。打开 SSH 连接后按提示输入用户名即可进入路由器配置界面。

```
login as: client002
Sent username "client002"
Trying public key authenticantion。
No passphrase required。

*********************************************************
*          All rights reserved (1997-2004)              *
*      Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*********************************************************

<Router>
```

⚠ 注意：

客户登录时输入的用户名应与路由器上配置的 **ssh user** *username* 命令中的 *username* 保持一致，否则无法建立连接。

11.7 哑终端服务

11.7.1 哑终端的功能描述

当路由器的异步口（如同/异步串口、AUX 口、八异步口）工作在流方式时，将微机（或终端）的串口与路由器异步口直连，可以进入路由器的命令行接口，对路由器进行配置，这称作哑终端工作方式。在哑终端基础上，可以建立其它应用，如执行 Telnet 命令登录其它设备。

用户在 PC 上运行超级终端可以与路由器任意一个异步口相连登录到路由器，对路由器进行配置管理。如下图所示。

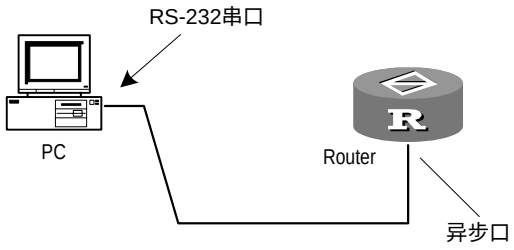

图11-11 哑终端连接方式

11.7.2 哑终端服务特性

参见表 11-2，与远程服务终端方式一致。

11.7.3 哑终端的典型应用

哑终端的典型应用方式：

- 异步口工作在流方式下，通过专线连接直接进入路由器的命令行接口，提供除 Console 口、Telnet 之外的另一种终端服务。
- 异步口工作在流方式下，通过异步专线直接登录到路由器的命令行接口，再启动 Telnet Client 客户端程序登录到其它远程系统上工作。

11.7.4 配置哑终端服务

与哑终端相关的配置命令如下表所示。请在接口视图下进行 **async mode** 命令的配置。请在用户界面视图下进行 **auto-execute command** 命令的配置。

表11-25 建立哑终端连接相关命令

操作	命令
设置异步接口的流方式	**async mode flow**
禁止异步接口的流方式	**async mode protocol**
在异步口上自动执行配置命令	**auto-execute command** *command*
在异步口上禁止自动执行配置命令	**undo auto-execute command**

1. 哑终端方式配置

配置与终端连接的异步口。

对同/异步口配置如下：

```
[Quidway-serial1/0/0] physical-mode async
[Quidway-serial1/0/0] async mode flow
```

对 8/16 异步口配置如下：

```
[Quidway-ui-tty1] undo modem
[Quidway-async1/0/0] async mode flow
```

对 AUX 口配置如下：

```
[Quidway-ui-aux0] undo modem
[Quidway-Aux0] async mode flow
```

在执行上述操作后，在该异步口的外接终端上键入两个回车，进入路由器的配置界面；在配置过程中，如果执行 quit 退出命令行界面，必须重新键入两个回车。

📖 说明：

其中异步口设置为禁止 Modem 拨入，是在相应的用户界面视图下完成的。具体内容详见用户界面配置章节。

---

2. auto-execute command 配置

如果在路由器的异步口配置了 **auto-execute command** 命令，那么，当用户在该异步口的外接终端上敲入两个回车后，路由器将自动执行某些命令，直接进入工作状态。

auto-execute command 命令使用时有如下的限制：

- 如果路由器上只有一个 Console 口或只有一个 AUX 口（Console 口和 AUX 口共一个口），那么这个口将不支持 **auto-execute command**。
- 如果路由器上有一个 Console 口和一个 AUX 口（共两个口）则 Console 口不支持 **auto-execute command**，AUX 口支持 **auto-execute command**。
- 对其它类型接口不作限制。

用户在登录时，自动执行某条在该终端上用 **auto-execute command** 配置好的命令，命令执行结束后，自动断开用户线。通常的用法，是在终端用 **auto-execute command** 配置 Telnet 命令，使用户自动连接到指定的主机。使用该命令，将导致不能用该终端线对本系统进行常规的配置，需谨慎使用。

⚠ 注意：

在配置 **auto-execute command** 命令并保存配置（执行 **save** 操作）之前，要确保可以通过其他手段登录系统，以去掉此配置。

---

auto-execute command 命令最典型的应用是用户以哑终端方式与路由器建立连接后，可以通过 **auto-execute command** 指定的 Telnet 命令再远程登录到其它路由器、主机或工作站上进行工作，这时，路由器对终端用户来说是透明的。如下图所示：

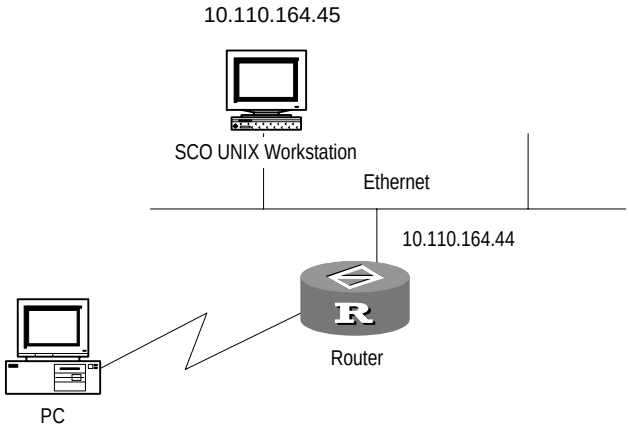

图11-12 auto-execute command 配置示意图

配置步骤：

将异步口（例如 serial1/0/0）配置成哑终端方式，参见上一小节配置。

配置 **auto-execute command** 命令。在用户界面视图下键入：

```
[Quidway-ui-vty0] auto-execute command telnet 10.110.164.45
```

配置完成后，在与路由器异步口相连的终端上敲入两次回车，直接登录到目的主机上。若退出目的主机，重新键入两个回车，再次登录到目的主机上。

📖 说明：

取消 **auto-execute command** 功能，在相应的用户界面视图下执行命令：**undo auto-execute command**。

11.7.5 哑终端连接的定时断开

请在用户界面视图下进行下列配置。

表11-26 哑终端连接的定时断开

操作	命令
允许定时断开哑终端连接	**idle-timeout** *minutes* [*seconds*]
恢复定时断开哑终端连接的默认值	**undo idle-timeout**

本功能是为了防止未授权用户的非法侵入。如果用户设置了 **idle-timeout**，在此时间内没有接收到哑终端用户的输入时，则断开与用户的连接。哑终端用户的定时断开时间为 10 分钟。用户可以在相应的用户界面视图下执行 **idle-timeout** 0 命令，关闭该功能。关闭该功能后，哑终端用户将永远不被断开。

禁止定时断开哑终端用户连接。

```
[Quidway-ui-vty0] idle-timeout 0
```

11.8 Remote Shell 服务

11.8.1 Remote Shell 介绍

Rsh（Remote Shell）最初为一个 Berkeley / UNIX 网络命令，用于在远程主机上执行特定的命令。远程主机需要运行有 Rsh 守护程序（Rsh Demon），支持 RSH 服务。Rsh 客户端与远程主机的守护进程通信。

Quidway 路由器实现 Rsh 客户端功能。下图所示为该特性的一种典型组网方式，用户可以在路由器上使用 RSH 命令远程执行服务器端主机上的命令。

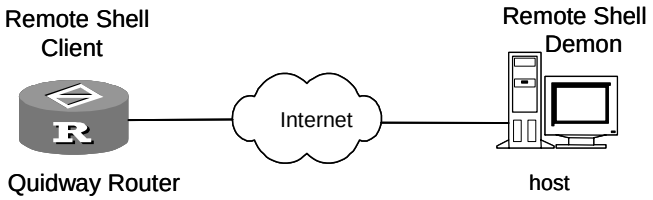

图11-13 Rsh 典型组网图

Rsh Demon 提供基于信任主机的特权端口认证的远程命令执行服务。在 Windows NT/2000/XP/2003 上都可以利用服务组件启动或关闭服务。

说明：

Windows NT/2000/XP/2003 系统不自带 Rsh Demon，需要安装 Rsh Demon 程序，然后才能启动此项服务。购买 Quidway 路由器不附带此软件，请用户自行购买或通过其它途径获取。

11.8.2 Rsh 客户端操作

Quidway 路由器作为 Remote Shell 客户端，使用命令行进行操作。

请在用户视图下进行下列操作。

表11-27 Rsh 客户端操作

操作	命令
Remote Shell 客户端操作命令	**rsh** *host* [**user** *username*] **command** *remote-command*

11.8.3 Rsh 调试

打开 **rsh** 命令的调试开关可以查看执行 **rsh** 命令后的运行情况，通过查看显示信息验证命令执行的效果。

请在用户视图下进行下列操作。

表11-28 Rsh 调试

操作	命令
打开 Rsh 调试开关	**debugging rsh**
关闭 Rsh 调试开关	**undo debugging rsh**

11.8.4 Rsh 客户端操作举例

如下图所示，Quidway 路由器作为 Remote Shell 客户端，远程主机为 Windows 2000 操作系统，已安装并启动了 Rsh Demon 服务。

通过路由器远程设置主机时间。

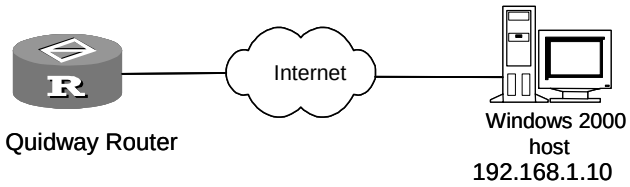

图11-14 Rsh 举例组网图

说明：

本例假设 Quidway 路由器和 Windows 2000 主机之间的路由可达。

---

1. 检查 Rsh Demon 在 Windows NT/2000/XP/2003 上是否安装和启动

(1) 进入 Windows 控制面板，打开“ 管理工具 ”。（对于 Windows XP 系统，当使用控制面板的分类视图时，在“ 性能和维护 ”类中选择“ 管理工具 ”。）

图11-15 Windows 管理工具文件夹视图

(2) 双击“服务”图标，进入 Windows“服务”管理窗口。

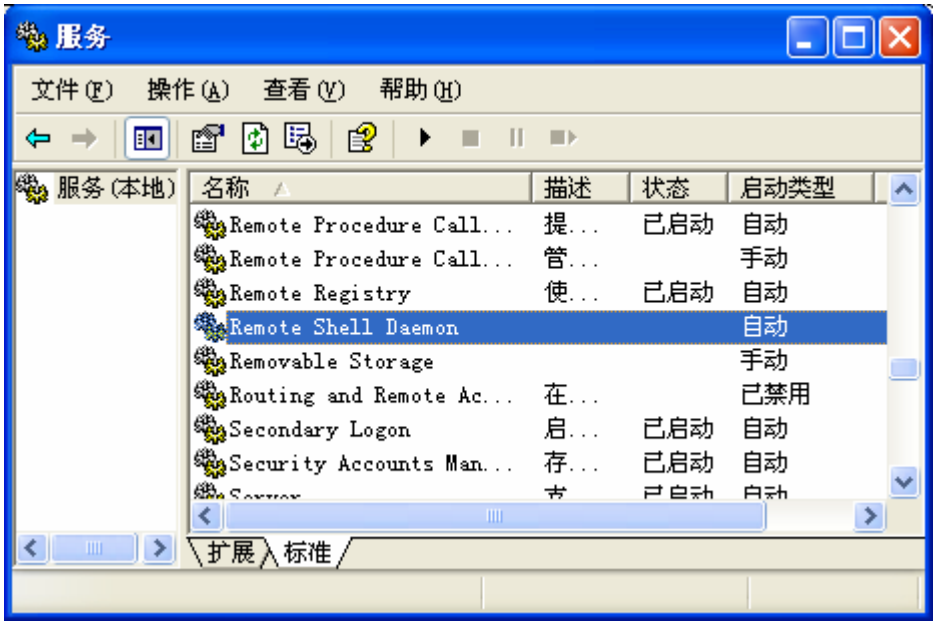

图11-16 Windows“服务”管理窗口

(3) 查找“服务”中是否包含“Remote Shell Daemon”。如果没有，说明尚未安装此服务程序，则需要先安装此程序。如果有，说明已经安装此服务程序。

(4) 查看是否启动“Remote Shell Daemon”服务。

如上图，在“Remote Shell Daemon”服务对应状态栏中可以查看该服务是否已经启动。本例中，该服务尚未启动。

(5) 启动“Remote Shell Daemon”服务。

双击该项服务，进入“ Remote Shell Daemon ”属性窗口，如下图。单击<启动>按钮，即可启动该项服务。

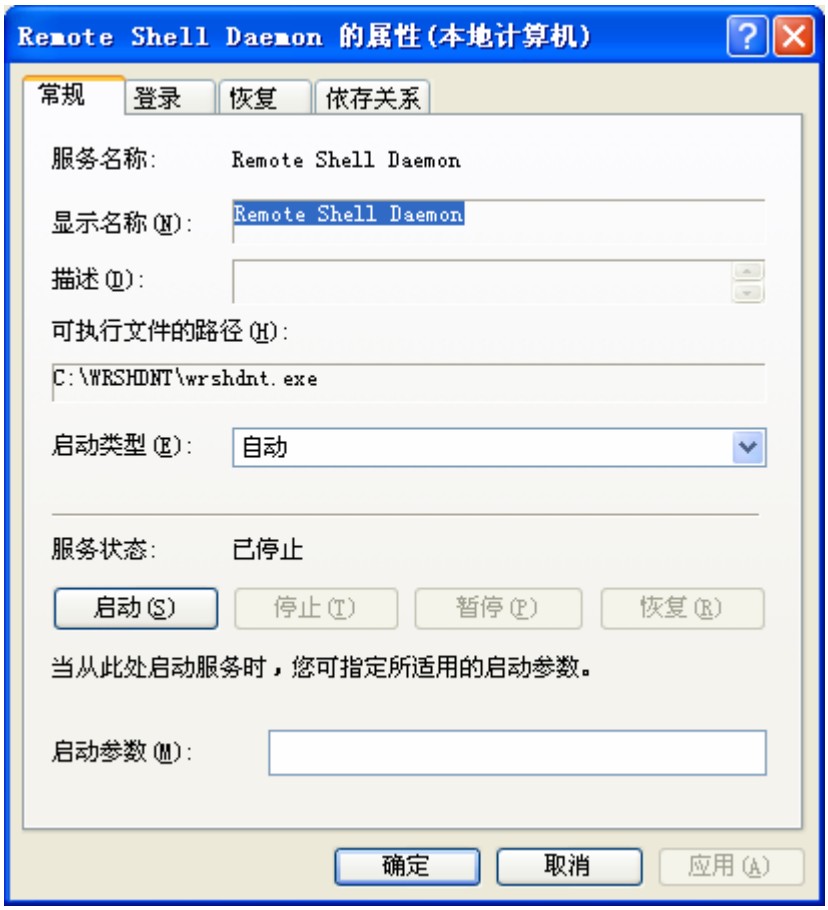

图11-17 “ Remote Shell Daemon ”属性窗口

2. 在路由器的用户视图下执行命令如下：

```
<Quidway> rsh 192.168.1.10 command time
Trying 192.168.1.10 ...
Press CTRL+K to abort
当前时间:  6:56:42.57
输入新时间: 12:00
12:00
```

11.9 Rlogin 终端服务连接

11.9.1 Rlogin 协议简介

Rlogin（Remote Login）协议最早来源于 Berkeley UNIX，是为该 UNIX 系统开发的一种远程登录服务，它比 Telnet 有更严格的控制和输出抑制能力，且该协议的实

现和使用更加简单。Rlogin 客户机和服务器之间使用 TCP 连接，提供多个终端远程登录到 UNIX 主机的功能。

VRP 实现的 Rlogin 服务是基于 Client 侧的，使路由器具有类似于多串口卡的功能——通过终端接入方式登录到路由器上的数字或模拟用户终端能够使用 Rlogin 协议登录到远端 UNIX 主机上。

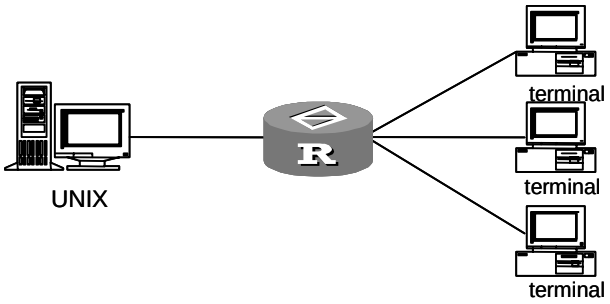

图11-18 通过路由器连接 UNIX Server 与 Terminal

路由器提供的 Rlogin（Client 端）具有下列特性：

- 支持的终端类型为 VT100。
- 支持的速率为 38400bps。
- 支持多种终端用户，如 Console 用户、AUX 用户、TTY 用户及 VTY 用户进行远端登录。
- 支持同一用户终端启动多个 Rlogin 会话的功能。

11.9.2 Rlogin 配置

请在用户视图下进行下列配置。

表11-29 建立 Rlogin 连接

操作	命令
建立 Rlogin 连接	**rlogin** *remote-host username*

11.9.3 Rlogin 的显示与调试

请在用户视图下进行下列配置。

表11-30 Rlogin 的显示与调试

操作	命令
打开 Rlogin 的调试开关	**debugging rlogin**
关闭 Rlogin 的调试开关	**undo debugging rlogin**

11.9.4 Rlogin 配置举例

1. 组网需求

用户 zhb 通过 Rlogin 登录到 IP 地址为 192.168.0.200 的 UNIX 服务器，在登录过程中，用户使用组合键“ ^K ”或本地终端命令“ . ”结束本地会话。

2. 组网图

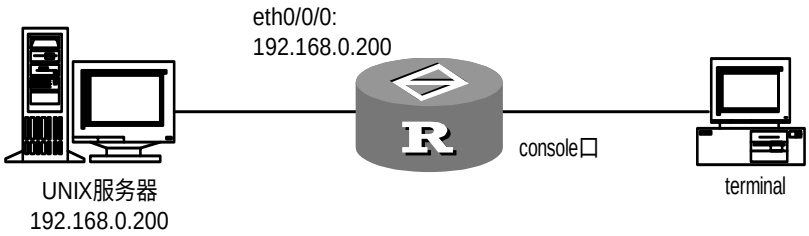

图11-19 Rlogin 配置举例

3. 配置步骤

(1) 配置 UNIX 服务器

增加用户 zhb（配置过程略）。

(2) 配置路由器

建立 Rlogin 连接。

```
<Quidway> rlogin 192.168.0.200 zhb
Trying 192.168.0.200 ...
Press CTRL+K to abort

Connected to 192.168.0.200 ...
Password:
Last login: Thu Oct 28 17:30:23 from 192.168.0.5
bash: Path: command not found
[root@localhost zhb] #
```

断开连接。

```
[root@localhost zhb] #   （输入“ ~ ”在接着输入句号“ . ”或者输入“ Ctrl+K ”）
The connection was closed by the local terminal!
```