基础配置

目 录

第 1 章 系统管理配置 1
1.1 配置文件管理 1
1.1.1 BSR28 文件系统概述 1
1.1.2 文件系统的管理 1
1.1.3 BSR28 启动流程图 2
1.1.4 文件系统命令 3
1.1.5 手工从某一文件中启动 4
1.1.6 通过命令从某一文件中启动 5
1.1.7 软件更新 5
1.1.8 配置更新 6
1.2 基本系统管理配置 7
1.2.1 配置以太网 IP 地址 7
1.2.2 配置缺省路由 7
1.2.3 利用 PING 测试网络连通状态 7
第 2 章 终端配置 9
2.1 VTY 配置说明 9
2.2 配置任务 9
2.3 监视与维护 10
2.4 配置举例 10
2.4.1 配置 TTY 举例 10
2.4.2 配置 VTY 举例 10
第 3 章 网络管理配置 11
3.1 配置 SNMP 11
3.1.1 概述 11
3.1.2 SNMP 配置任务列表 12
3.1.3 SNMP 配置任务 12
3.1.4 配置实例 16
3.2 配置 RMON 16
3.2.1 配置 RMON 配置任务列表 16
3.2.2 配置 RMON 配置任务 17
3.3 配置 PDP 20
3.3.1 概述 20
3.3.2 PDP 配置任务列表 20
3.3.3 PDP 配置任务 20
3.3.4 监控和管理 PDP 21
3.3.5 PDP 配置实例 21

第 4 章 Ssh 配置 22
4.1 SSH 概述 22
4.1.1 SSH server 22
4.1.2 SSH client 22
4.1.3 实现特性 22
4.2 配置任务 22
4.2.1 配置认证方法列表 22
4.2.2 配置授权方法列表 22
4.2.3 配置认证方式 23
4.2.4 配置静默时间 23
4.2.5 配置 aes 23
4.2.6 配置最大用户数 23
4.2.7 配置文件下载功能 23
4.2.8 配置压缩功能 24
4.2.9 配置压缩等级 24
4.2.10 配置访问列表 24
4.2.11 配置认证超时时长 24
4.2.12 配置认证重试次数 24
4.2.13 使能 ssh server 25
4.3 Ssh server 配置示例 25
4.3.1 访问控制列表 25
4.3.2 全局配置 25

第1章　系统管理配置

1.1　配置文件管理

1.1.1　BSR28 文件系统概述

BSR28 路由器上的存储设备，共有三种配置形式：

1) 只有 Flash

2) 只有 CF 卡

3) 同时存在 Flash 和 CF 卡

Flash 与 CF 卡的关系地位，就如同 windows 操作系统中的 C 盘，D 盘的概念，系统可以安装在 C 盘，也可以安装在 D 盘。路由器上所必备的可执行文件（一般扩展名为 BIN）和配置文件（startup-config）既可以放在 Flash 中，也可以放在 CF 卡中。Flash 就如同 windows 中的 C 盘，一般默认将上述两个文件存放在 Flash 中，除非路由器上只存在 CF 卡，或是希望主要使用 CF 卡时，才将文件存放到 CF 卡中。

1.1.2　文件系统的管理

FLASH 以及 CF 卡中文件的名字最长只能有 20 个字符，且不区分大小写。

U 盘文件系统只能为 FAT16 或 FAT32，文件名应符合 DOS 的 8.3 格式，即名字最长为 8 个字符，扩展名最长为 3 个字符，字符只能由英文和数字组成，且英文字符不区分大小写。

1.1.3 BSR28 启动流程图

1. 上电启动流程

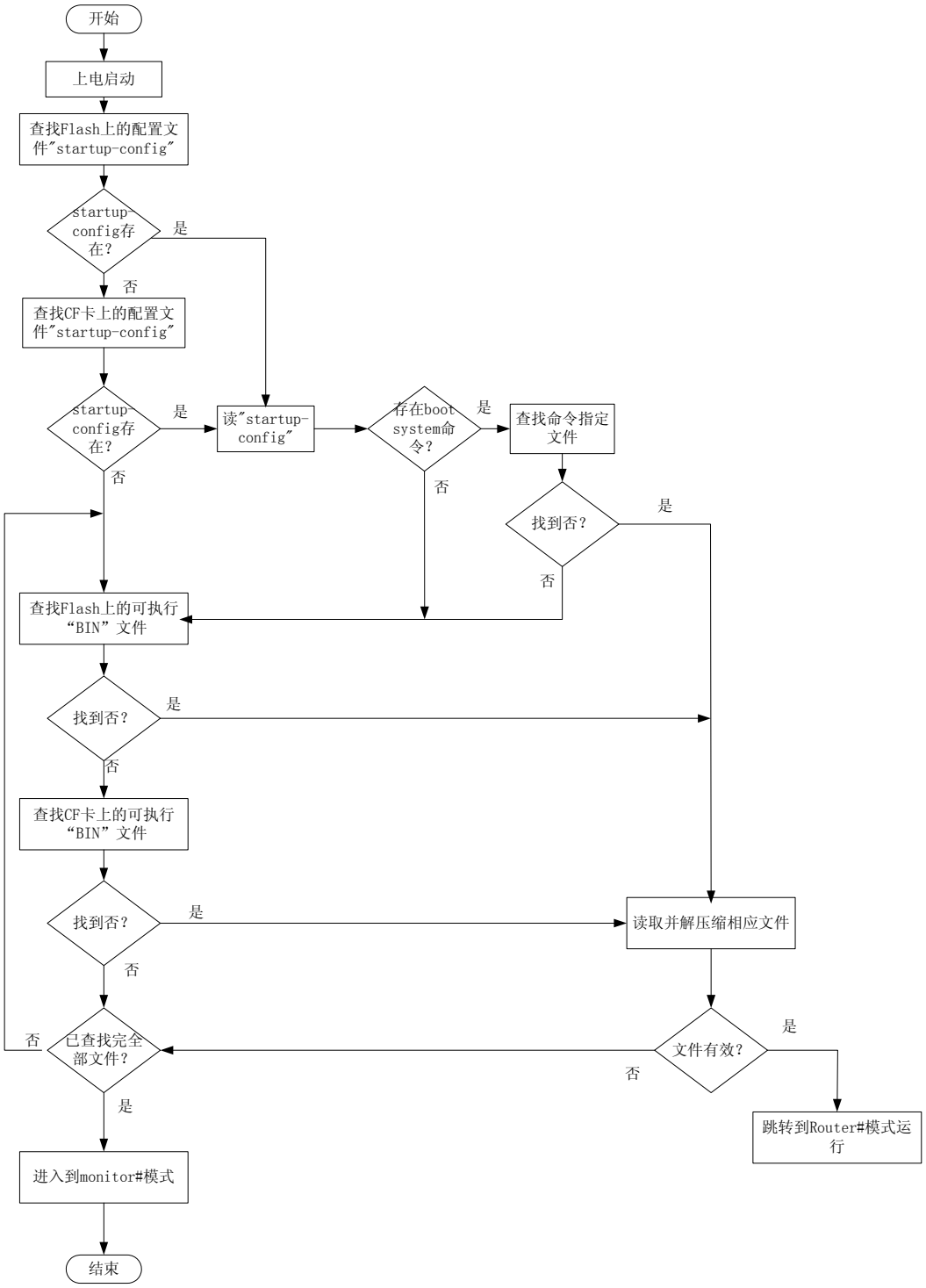

图 1-1

2. Router#运行流程图

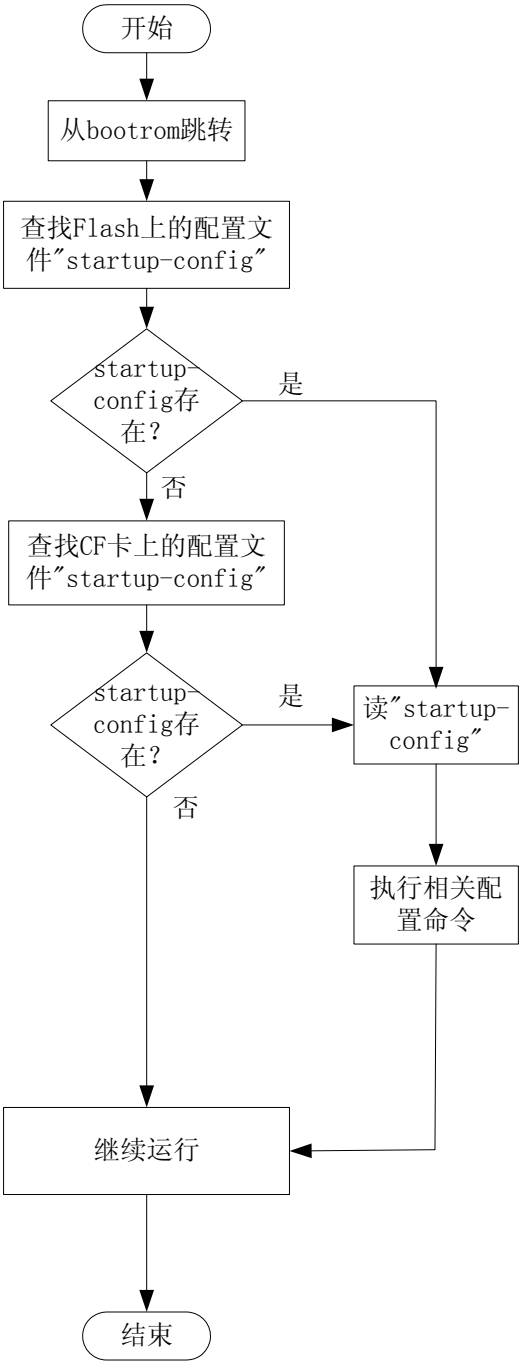

图 1-2

1.1.4 文件系统命令

所有命令黑体字部分为关键字，其余为参数。[]内的部分是可选配置。

- **pwd**

  显示当前工作目录。

- **dir** [目录名]

  显示文件和目录名。[]内目录名需要使用绝对路径，若为当前工作目录子目录，则可省略路径。文件显示的格式如下：

  [索引号] 文件名 <FILE> 文件长度 创立时间

  缺省显示当前工作目录下的文件。

- **write**

  保存当前配置。命令执行后生成的 startup-config 文件将保存于当前工作目录下。

- **format** [存储设备的根目录名]

  格式化文件系统，删除所有数据。

- **delete** [文件名]

  删除一个文件，如果文件不存在，提示该文件不存在，缺省删除当前工作目录下的 startup-config。

- **more** 文件名

  显示某个文件的内容，如果文件不存在，提示该文件不存在。

- **rename** 文件名 新文件名

  重命名某个文件

- **cd** 目录名

  改变当前工作目录。目录名需要使用绝对路径，若为当前工作目录子目录，则可省略路径。

- **rd**

  删除一个目录

- **md**

  创建一个目录

1.1.5 手工从某一文件中启动

monitor#boot flash <local_filename>

本命令是用来启动 flash 闪存中的某个路由器软件，闪存中可能存有多个路由器软件；

monitor#boot cf <local_filename>

本命令是用来启动 CF 卡闪存中的某个路由器软件，闪存中可能存有多个路由器软件。

参数说明

参数	参数说明
local_filename	存于闪存中的文件名，用户必须输入文件名。

举例

monitor#boot flash router.bin

若 flash 闪存中存在 router.bin 文件，则开始读取 router.bin，并解压启动;

monitor#boot cf router.bin

若 CF 卡闪存中存在 router.bin 文件，则开始读取 router.bin，并解压启动;

1.1.6 通过命令从某一文件中启动

Router_config#boot system flash <local_filename>

此命令是用来在路由器上电时，指定从 Flash 闪存中的某个路由器软件启动，闪存中可能存有多个路由器软件。

Router_config#boot system cf <local_filename>

此命令是用来在路由器上电时，指定从 CF 卡闪存中的某个路由器软件启动，闪存中可能存有多个路由器软件。

配置完上述命令后，需执行"write"，将配置保存，才能在重新启动的时候生效。

参数说明

参数	参数说明
local_filename	存于闪存中的文件名，用户必须输入文件名。

举例

Router_config#boot system cf router.bin

配置保存后，如果 CF 卡中有 router.bin 文件，重新启动时系统就会从这个文件启动

1.1.7 软件更新

用户可使用本命令从本地或远程下载路由器系统软件， 以获得版本升级或您向本公司定制的特殊功能版本(如数据加密等)。

监控状态下软件更新有两种方式。

1. 通过 TFTP 协议

monitor#copy tftp<:*filename*> flash <:*filename*> [ip_addr]

本命令是用来从 tftp 服务器拷贝文件到系统的 flash 闪存，用户键入命令后，系统会提示用户输入远端服务器名和远端的文件名。

monitor#copy tftp<:*filename*> cf <:*filename*> [ip_addr]

本命令是用来从 tftp 服务器拷贝文件到系统的 CF 卡闪存，用户键入命令后，系统会提示用户输入远端服务器名和远端的文件名。

参数说明

参数	参数说明
tftp<:filename>	表示从TFTP服务器读取文件。filename指明相应的文件名，若没有指定，copy命令执行后将提示用户将文件名输入。
flash <:filename>	表示向路由器flash闪存中写文件。filename指明相应的文件名，若没有指定，copy命令执行后将提示用户将文件名输入。
cf <:filename>	表示向路由器CF卡闪存中写文件。filename指明相应的文件名，若没有指定，copy命令执行后将提示用户将文件名输入。
ip_addr	Tftp 服务器的IP地址。若没有指定，copy命令执行后将提示用户输入。

举例

从服务器读名为“main.bin”的文件，写入路由器叫“router.bin”

monitor#copy tftp flash:router.bin

提示：Remote-server ip address[]?192.168.0.116

提示：Name of remote file to read[]?main.bin

TFTP:successfully receive 36 blocks ,18370 bytes
monitor#

1.1.8 配置更新

路由器配置以文件形式保存，文件名为 startup-config，用户可以使用与软件更新类似的命令来更新配置。

1. 通过 TFTP 协议

monitor#copy tftp flash:startup-config

monitor#copy tftp cf:startup-config

1.2 基本系统管理配置

1.2.1 配置以太网 IP 地址

monitor#ip address <ip_addr> <net_mask>

本命令是用来配置以太网 IP 地址,系统缺省为 192.168.0. 1,网络掩码为 255.255.255.0

参数说明

参数	参数说明
ip_addr	以太网IP地址。
net_mask	以太网网络掩码。

举例

monitor#ip address 192.168.1.1 255.255.255.0

1.2.2 配置缺省路由

monitor#ip route default <ip_addr>

本命令是用来配置缺省路由，只能配置一条缺省路由。

参数说明

参数	参数说明
ip_addr	网关的IP地址。

举例

monitor#ip route default 192.168.1.1

1.2.3 利用 PING 测试网络连通状态

monitor#ping <ip_address>

本命令是用来测试网络连通状态。

参数说明

参数	参数说明
ip_address	目的IP地址。

举例

```
monitor#ping 192.168.0.100
Reply from 192.168.0.100 : data=48, time=10ms, ttl=128
Reply from 192.168.0.100 : data=48, time=10ms, ttl=128
Reply from 192.168.0.100 : data=48, time=10ms, ttl=128
Reply from 192.168.0.100 : data=48, time=10ms, ttl=128
4 packets sent, 4 packets received
round-trip min/avg/max = 0/2/10 ms
```

第2章　终端配置

2.1　VTY配置说明

路由器使用 line 命令配置终端参数，简单、灵活；配置过程符合用户的使用习惯；在 line 命令中可对终端显示的宽度、高度等设置。

2.2　配置任务

路由器有四种类型的线路：控制台，辅助，异步和虚拟终端线路。不同路由器有不同数量的这些类型的线路。参考下面的软件和硬件配置指南使设备有正确的配置。

线路类型	接口	描述	线路编号规则
CON(CTY)	控制台	用于登录到路由器进行配置服务。	编号0。
AUX	辅助	RS-232 DTE端口。用作备份的异步端口(TTY). 不能被用作第二个控制台端口。	编号：少于（或等于）4个插槽为65，否则为插槽数乘以16加一。
TTY	异步	就是异步接口。常用于使用SLIP,PPP的远程接点的拨入会话。	起始编号为1。编号数量随平台不同而变化。编号范围为路由器所支持的最大数量的异步接口。例如，在1号槽插有16异步模块，2号槽空缺，3号槽为8同步模块，这样a1/0对应line 1，a1/15对应line 16，s3/0对应line 17，s3/7对应line 24。
VTY	虚拟异步	用于连接到路由器上的同步端口[如以太网和串行接口]的Telnet,X.25 PAD、HTTP和Rlogin等。	从最大TTY线路号加一开始的64个编号。

1. 线路和接口之间的关系

- 异步接口和 TTY 线路
- 同步接口和 VTY 线路

异步接口和 TTY 异步接口对应于物理终端线路[TTY]。当异步接口不封装协议，可接终端。

同步接口和 VTY 线路：虚拟终端线路提供了通过同步接口对路由器进行的访问。VTY 线路不象 TTY 线路对于异步接口那样对应于同步接口。这是因为 VTY 线路在路由器中被动

态建立，然而 TTY 线路是静态的物理端口。当一个用户通过 VTY 线路连接到路由器时，用户正在连接至一个接口上的虚拟端口。对于每一个同步接口都可以有多个虚拟端口。

例如，几个 Telnet 连接到一个接口[Ethernet 或串行接口]。

VTY 配置需做如下工作：

- 进入行配置模式
- 对终端参数配置

2.3 监视与维护

用 show line 命令查看 VTY 的配置。

2.4 配置举例

2.4.1 配置 TTY 举例

下面配置在 tty1-tty10 上设置终端输出行宽及终端的每屏输出行数，用户从该端口登陆，每 40 行出现 more 提示；行宽超过 132 个字符则换行；

```
config#line tty 1 10
config_line#width 132
config_line#length 40
```

下面配置将 A1/0 设为 TTY 端口。

```
config_A1/0#async mode interactive
```

这样的配置是使用直接的背靠背线缆与 A1/0 端口相连。

2.4.2 配置 VTY 举例

下面配置将取消所有 VTY 的每屏输出行数限制，不出现 more 提示

```
config#line vty 0 63
config_line#length 0
```

第3章　网络管理配置

3.1　配置SNMP

3.1.1　概述

SNMP 系统包括下面 3 个部分：

- SNMP 管理端 (NMS)
- SNMP 代理 (AGENT)
- 管理信息库 （MIB）

SNMP 是应用层协议。它提供了在 SNMP 管理端和代理之间进行通信的报文格式。

SNMP 管理端可以是网络管理系统（NMS，如 CiscoWorks）的一部分。代理和 MIB 驻留在路由器上。配置路由器上的 SNMP，需要定义管理端和代理间的关系。

SNMP 代理包含 MIB 变量，SNMP 管理端可以查询或改变这些变量的值。管理端可以从代理处得到变量值，或者把变量值存储到代理处。代理从 MIB 收集数据。MIB 是设备参数和网络数据的信息库。代理也能响应管理端的读取或设置数据的请求。SNMP 代理可以主动向管理端发送陷阱（trap）。陷阱是针对网络的某一条件而向 SNMP 管理端报警的消息。陷阱能指出不正确的用户认证、重启、链路状态（启动或关闭）、TCP 连接的关闭、与邻近路由器连接的丢失或其它重要的事件。

1. SNMP 通告

特殊事件发生时路由器能向 SNMP 管理端发送通知(inform)。例如，当代理路由器遭遇一个错误条件时，它可能向管理端发送一个消息。

SNMP 通告可以作为陷阱（Trap）或通知请求（inform request）来发送。由于接收方收到一个陷阱时不发送任何应答，导致发送方不能确定是否陷阱已经被接收，所以陷阱不可靠。与此相对的是，接收通知请求的 SNMP 管理端用 SNMP 响应 PDU 作为这个消息的应答。如果管理端没有收到一个通知请求，也不会发送响应。如果发送方没有收到应答，那么可以重新发送通知请求。这样，通告更可能到达它们计划中的目的地。

因为通知请求更加可靠，所以它们消耗了路由器和网络的更多的资源。陷阱只要一发出便被丢弃。与此不同的是，通知请求必须保留在内存中，直到收到响应或者请求超时。另外，陷阱只发送一次，而通知请求可以重新发送多次。重新发送增加了网络通信量并在网络上产生更多的负荷。因此，陷阱和通知请求在可靠性和资源间提供了平衡。如果 SNMP 管理端非常需要收到每个通知，可使用通知请求；如果关心网络的通信量或路由器的内存，并且不必收到每个通知，可使用陷阱。

本公司路由器目前支持陷阱，但提供了对通知请求的扩充。

2. SNMP 的版本

本公司路由器现支持下面的 SNMP 版本：

- SNMPv1---简单网络管理协议，一个完全的 Internet 标准，在 RFC1157 中定义。
- SNMPv2C--- SNMPv2 的基于团体的管理框架，Internet 试验协议，在 RFC1901 中定义。

本公司路由器将支持下面版本的 SNMP：

- SNMPv3

SNMPv1 使用基于团体的安全形式。能访问代理 MIB 的管理端团体用 IP 地址访问控制列表和口令来定义。

必须把 SNMP 代理配置为管理工作站支持的 SNMP 版本。代理能与多个管理端通信。

3. 所支持的 MIB

本公司路由器的 SNMP 支持所有的 MIB II 变量（在 RFC 1213 中讲述）和 SNMP 陷阱（RFC 1215 中讲述）。

本公司路由器为每个系统提供了自己私有的 MIB 扩充。

3.1.2 SNMP 配置任务列表

- 为 SNMP 团体创建或修改访问控制
- 设置该路由器管理员的联系方法和路由器所在位置
- 定义 SNMP 代理数据包的最大长度
- 监视 SNMP 状态
- 配置 SNMP 陷阱
- 配置 SNMPv3 属性

3.1.3 SNMP 配置任务

1. 为 SNMP 团体创建或修改访问控制

使用 SNMP 团体字符串定义 SNMP 管理端和代理的关系。团体字符串类似于允许访问路由器上代理的口令。可选的是，可以指定下面一个或多个与团体字符串相关联的特性：

- 允许使用团体字符串获得代理访问权的 SNMP 管理端的 IP 地址访问列表。

- 定义对指定团体有访问权的所有 MIB 对象子集的 MIB 视图。
- 指定团体对有访问权的 MIB 对象的读写权限。

在全局配置模式下使用下面的命令来配置团体字符串：

命令	目的
snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*word*]	定义团体访问字符串。

可以配置一个或多个团体字符串。使用 no snmp-server community 命令除去给定的团体字符串。

2. 设置该路由器管理员的联系方法和路由器所在位置

sysContact 和 sysLocation 都是 MIB 中 system 组中的管理变量，分别定义了被管理该节点（路由器）的联系人标识和实际位置。这些信息可以通过配置文件进行访问。在全局配置模式下使用下面的一个或多个命令：

命令	目的
snmp-server contact *text*	设置节点联系人字符串。
snmp-server location *text*	设置节点位置字符串。

3. 定义 SNMP 代理数据包的最大长度

当 SNMP 代理接收请求或发出响应时，可以设置数据包的最大许可长度。在全局配置模式下使用下面的命令：

命令	目的
snmp-server packetsize *byte-count*	设定数据包的最大许可长度。

4. 监视 SNMP 状态

在全局配置模式下使用下面的命令，监视 SNMP 输入和输出统计，包括非法团体字符串条目，错误和请求变量的数量。

命令	目的
show snmp	监视SNMP状态。

5. 配置 SNMP 陷阱

使用下面的命令配置路由器发送 SNMP 陷阱（第二个任务是可选的）：

- 配置路由器发送陷阱
- 改变陷阱运行参数

配置路由器发送陷阱

在全局配置模式下使用下面的命令配置路由器向一个主机发送陷阱。

命令	目的
snmp-server host host *community-string* [*trap-type*]	指定陷阱消息的接受者。
snmp-server host *host* [traps|informs]{version {v1 | v2c | v3 {auth | noauth | priv } }}*community-string* [*trap-type*]	指定陷阱消息的接受者，以及陷阱信息的版本号和用户名等 注意：对于SNMPv3的陷阱，在配置接收陷阱的主机之前必须为该主机配置SNMP引擎ID。

路由器开机后，SNMP 代理自动启动，所有类型的陷阱被激活。使用 snmp-server host 命令指定哪个主机将要接收哪些类型的陷阱。

有些陷阱需要通过其它命令来控制。例如，如果要在接口打开或关闭时会发送 SNMP 链路陷阱，需在接口配置模式下使用 snmp trap link-status 激活链路陷阱。使用接口配置命令 no snmp trap link-stat 关闭这些陷阱。

为了使主机收到陷阱，必须为该主机配置 snmp-server host 命令。

改变陷阱运行参数

作为可选项，可以指定产生陷阱的源接口，指定发送 Trap 的目的端口，为每个主机指定消息（数据包）队列长度或重发间隔的值。

在全局配置模式下使用下面可选命令改变陷阱运行参数：

命令	目的
snmp-server trap-source *interface*	指定产生陷阱消息的源接口。该命令为信息也设置源IP地址。
snmp-server queue-length *length*	为每个陷阱主机建立消息队列长度。 缺省为10。
snmp-server trap-timeout *seconds*	定义重发队列中重发陷阱消息的频率。 缺省为30秒。
snmp-server udp-port *seconds*	指定Trap发送的端口号

6. 配置 SNMPv3 属性

SNMPv3 属性包括一下配置：

- 配置 SNMPv3 组
- 配置 SNMPv3 用户

- 配置 SNMPv3 引擎 ID

配置 SNMPv3 组

通过下面的命令配置组

命令	目的
snmp-server group [*groupname* {**v1** | **v2c** |**v3** [**auth** | **noauth** | **priv**]}][**read** *readview*][**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	配置一个SNMPv3组。默认情况下可以读internet子树下所有叶子，不可以写任何叶子。

配置 SNMPv3 用户

通过下面的命令配置一个本地用户，管理者访问设备时，必须使用设备上配置的用户名和密码进行访问。用户的安全级别不能低于用户所属的组的安全级别，否则用户不能通过认证

命令	目的
snmp-server user username groupname {v1 | v2c | v3 [encrypted] [auth {md5 | sha} *auth-password* **]} [access** *access-list***]**	配置一个本地SNMPv3用户

通过下面的命令配置一个远端用户，设备需要向远端管理站发送 Trap 类报文时，如果管理站需要进行身份认证，则需要配置远程用户。远程用户的用户名和口令的配置必须与管理站上的配置一致，否则管理站不能接收到 Trap 报文。

命令	目的
snmp-server user username groupname remote *ip-address* **[udp-port** *port***] {v1 | v2c | v3 [encrypted] [auth {md5 | sha}** *auth-password* **]} [access** *access-list***]**	配置一个远程SNMPv3用户 注意：配置远程用户之前，需要先为该IP地址的管理站配置一个远程SNMP引擎ID

配置 SNMPv3 引擎 ID

SNMP 引擎 ID 用于标识一个 SNMP 引擎。传统的 SNMP 管理者和代理者在 SNMPv3 框架中都是 SNMP 引擎的一部分

命令	目的
snmp-server engineID remote *ip-address* **[udp-port** *port-number***]** *engineid-string*	配置远端SNMP引擎。

3.1.4 配置实例

例 1

```
snmp-server community public RO
snmp-server community private RW
snmp-server host 192.168.10.2 public
```

在这个例子中配置了对所有 MIB 变量有读权限的团体字符串 public 与对所有 MIB 变量有读写权限的团体字符串 private。用户可以用团体字符串 public 读路由器中 MIB 变量，用 private 读路由器中的 MIB 变量与写路由器中可写的 MIB 变量。它还指定了当路由器需要发送陷阱消息时，用团体字符串 public 向 192.168.20.2 发送陷阱消息。例如当路由器的某个端口 down 时，路由器会向 192.168.20.2 发送一条 linkdown 的陷阱消息。

例 2

```
snmp-server community public view sysmib RO
snmp-server community private RW nativehost
snmp-server contact router@company.com.cn
snmp-server host 192.168.10.2 public snmp
snmp-server location 405-room
snmp-server view sysmib system included
ip access-list standard nativehost
permit 192.168.10.2 255.255.255.255
```

在这个例子中团体字符串 public 只对路由器中系统组的 MIB 变量有读的权限，只允许 IP 地址为 192.168.10.2 的主机用团体字符串 private 读写路由器中的 MIB 变量。对主机 192.168.10.2 只发送 snmp 陷阱消息，而不发送 authentication 或 configure 陷阱消息。将联系方式设为 router@company.com.cn，位置设为 405-room，也就是说系统组的 MIB 变量 sysContact 的值为 router@company.com.cn ，sysLocation 的值为 405-room。

3.2 配置RMON

3.2.1 配置 RMON 配置任务列表

- 配置路由器 RMON 告警功能
- 配置路由器 RMON 事件功能
- 配置路由器 RMON 统计功能
- 配置路由器 RMON 历史功能
- 显示路由器 RMON 配置

3.2.2 配置 RMON 配置任务

1. 配置路由器 RMON 告警功能

可以通过命令行或 SNMP 网管配置 RMON 告警功能；如果通过 SNMP 网管配置，还需要对路由器的 SNMP 进行配置。告警功能使能后，设备可以监控系统中某些统计值。配置 RMON 告警功能步骤如下：

命令	目的
configure	进入全局配置模式。
rmon alarm *index variable interval* {absolute | delta} rising-threshold *value* [*eventnumber*] **falling-threshold** *value* [*event number*] [**owner** *string*]	增加一个rMon告警表项 ● index为该表项的索引，有效范围1~65535。 ● variable为被监测MIB中对象，必须是系统中一个有效的MIB对象，并且只有类型为INTEGER、Counter、Gauge或TimeTicks的对象才能被检测。 ● interval为取样的间隔时间，以秒为单位，有效范围1~4294967295。 ●使用absolute来直接监测MIB对象的取值；适用delta来监测两次取样之间MIB对象值的变化。 ●value用于表示产生告警的阈值，对应的eventnumber表示到达该阈值时产生的事件的索引；eventnumber是可选的。 ● owner string可以用来描述该告警的一些描述性信息。
exit	退回到管理模式。
write	保存配置

配置完成一条告警表项后，设备会每隔 interval 秒获取 variable 指定的 OID 的值，并根据告警类型（absolute 或 delta）与前次值进行比较，如果本次统计值比前次大并且超出 rising-threshold 指定的阈值则会引发索引为 eventnumber 的事件（如果 eventnumber 为零或事件表不存在索引为 eventnumber 的事件则不引发），下降亦然；如果无法获取 variable 指定的 OID，则本行告警表项状态被设置为 invalid。当使用 rmon alarm 命令多次配置相同 index 的告警表项时，只有最后一次配置的参数有效；使用 no rmon alarm index 命令删除索引为 index 的告警表项。

2. 配置路由器 RMON 事件功能

配置 RMON 事件步骤如下：

命令	目的
configure	进入全局配置模式
rmon event *index* [**description** *string*] [**log**]	增加一个RMON事件表项：

[**owner** *string*] [**trap** *community*]	● index为该表项的索引，有效范围1~65535。 ● description表示该事件的描述信息。 ●log表示该事件被引发时在log表中增加一条信息。 ●Trap 表示该事件被引发时产生一条 trap，community为团体名称。 ● owner string可以用来描述该事件的一些描述性信息。
exit	退回到管理模式。
write	保存配置 。

配置 RMON 事件后，当触发 RMON 告警时，首先更新本事件表项的 eventLastTimeSent 域为当时的 sysUpTime；如果该事件配置了 log 属性，则向 log 表中增加一条信息；如果配置了 Trap 属性，则以 community 为团体名称发出一条 trap。当使用 RMON event 命令多次配置相同 index 的事件表项时，只有最后一次配置的参数有效；使用 no rmon event index 命令删除索引为 index 的事件表项。

3. 配置路由器 RMON 统计功能

RMON 统计组用于监测设备上每一个接口上的统计信息。RMON 统计功能配置步骤如下：

命令	目的
configure	进入全局配置模式。
interface *iftype ifid*	进入端口模式： ● iftype为端口的类型 ●ifid为接口的ID
rmon collection stat *index* [**owner** *string*]	在该接口上使能统计功能 ● index为统计表项索引； ● owner string可以用来描述该统计表的一些描述性信息。
exit	退回到全局模式。
exit	退回到管理模式。
write	保存配置。

当使用 rmon collection stat 命令多次配置相同 index 的事件表项时，只有最后一次配置的参数有效；使用 no rmon collection stats index 命令删除索引为 index 的统计表项。

4. 配置路由器 RMON 历史功能

RMON 历史组用于收集设备上一个接口上的不同时间段的统计信息。rMon 统计功能配置步骤如下：

命令	目的
configure	进入全局配置模式
interface *iftype ifid*	进入端口模式：iftype为端口的类型；ifid为接口的ID。
rmon collection history *index* [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]	在该接口上使能历史功能 ● index为该历史表项索引； ● 在所有该历史记录控制表项收集的数据中，最近bucket-number条表项需要保留，用户可以浏览以太网历史记录表获取这些统计值；默认值为50条 ● second为每两次获取统计数据的间隔时间，默认值为1800秒（半小时） ●owner string可以用来描述该历史控制表的一些描述性信息
exit	退回到全局模式。
exit	退回到管理模式。
write	保存配置。

增加一个历史控制表项后，设备会每隔 second 秒从指定的接口上获取一次统计值，将结果作为表项增加到以太网历史记录表中。当使用 rmon collection history index 命令多次配置相同 index 的历史表项时，只有最后一次配置的参数有效；使用 no rmon history index 命令删除索引为 index 的历史控制表项。注意 bucket-number 过大和 interval second 过小都会过多占用系统资源。

5. 显示路由器 RMON 配置

使用 show 命令显示路由器 RMON 配置：

命令	目的
show rmon [**alarm**] [**event**] [**statistics**] [**history**]	显示RMON配置信息： ● alarm表示显示告警表项配置。 ● event表示显示事件表项配置，同时显示由于事件被引发而导致log表中包含的表项。 ● statistics表示显示统计表项配置，同时显示设备收集到的该接口上的统计值。 ● history表示显示历史表项配置，同时显示设备收集到的该接口上最近指定个数时间间隔内的统计值。

3.3 配置PDP

3.3.1 概述

PDP 协议专门用于发现网络设备的两层协议，用于网管程序发现已知设备的所有邻居，使用 PDP，能够学到邻居设备的设备类型和 SNMP 代理地址。通过 PDP 发现邻居设备，网管程序能够用 SNMP 询问邻居设备以获得网络拓扑结构。

本公司路由器上的 PDP 功能能够实现发现邻居设备的功能，但不能接受 SNMP 询问邻居设备，所以，路由器只能处于网络边缘，否则，将不能获得完整的网络拓扑结构。

路由器上的 PDP 能够配置于所有的 SANP 上（如以太网、HDLC、帧中继、PPP）。

路由器 PDP 默认配置如下：

功能	默认设置
PDP全局配置状态	未启动。
PDP端口配置状态	未启动
PDP时钟（发送报文频率）	60秒
PDP信息保存	180秒

3.3.2 PDP 配置任务列表

- 设置 PDP 时钟和信息保存时间
- 启动路由器上的 PDP
- 启动路由器端口上的 PDP

3.3.3 PDP 配置任务

1. 设置 PDP 时钟和信息保存时间

设置 PDP 发送报文的频率和 PDP 信息保存时间时，可以在全局配置模式下使用下面的命令：

命令	目的
pdp timer *seconds*	配置PDP发送报文的频率。
pdp holdtime *seconds*	配置PDP信息保存时间。

2. 启动路由器上的 PDP

PDP 在默认配置下是没有启动的，如果要使用 PDP，可以在全局配置模式下使用下面的命令：

命令	目的
pdp run	启动路由器上的PDP功能。

3. 启动路由器端口上的 PDP

PDP 在默认配置下是没有启动的，当启动路由器上的 PDP 后，可以在端口上启动 PDP，在接口配置模式下使用下面的命令：

命令	目的
pdp enable	启动路由器端口上的PDP功能。

3.3.4 监控和管理 PDP

为了监控 PDP，可以在管理模式下使用下面的命令：

命令	目的
show pdp traffic	显示路由器接收和发送的PDP报文计数。
show pdp neighbor [*detail*]	显示路由器通过PDP发现的邻居。

3.3.5 PDP 配置实例

1. 启动 PDP 功能

```
Router_config# pdp run
Router_config# int f0/0
Router_config_f0/0#pdp enable
```

2. 配置 PDP 时钟和信息保存时间

```
Router_config# pdp timer 30
Router_config# pdp holdtime 90
```

3. 监控 PDP 信息

```
router#  show pdp neighbors
Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H -
Host, I - IGMP, r - Repeater
Device ID Local IntrfceHoldtmeCapabilityPlatform Port ID
joeEth 0 133 4500 Eth 0
samEth 0 152 R AS5200 Eth 0
```

第4章 Ssh 配置

4.1 SSH概述

4.1.1 SSH server

SSH client 通过 SSH server 和设备建立安全的、加密的通信连接。该连接提供和 telnet 相似的功能。SSH server 支持的加密算法包括 des、3des 和 blowfish，支持的压缩算法包括 zlib。

4.1.2 SSH client

SSH client 是运行于 ssh 协议之上，提供认证和加密特性的应用。由于使用了认证和加密，SSH client 允许通信设备之间或者和其他支持 SSH server 的设备之间在不安全的网络环境中建立安全的通信。SSH client 支持的加密算法包括 des，3des 和 blowfish。

4.1.3 实现特性

ssh server 和 ssh client 支持 ssh 版本 1.5，2.0。在功能特性上，只支持 shell 应用。

4.2 配置任务

4.2.1 配置认证方法列表

ssh server 使用 login 认证方式，缺省情况下使用名为“default”的认证方法列表。

在全局配置态下使用下面的命令配置认证方法列表：

命令	目的
ip sshd pwd-method authentication-list STRING	配置认证方法列表。

4.2.2 配置授权方法列表

ssh server 缺省情况下使用名为“default”的授权方法列表。

在全局配置态下使用下面的命令配置授权方法列表：

命令	目的
ip sshd pwd-method authorization-list	配置授权方法列表。

STRING	

4.2.3 配置认证方式

ssh server 缺省情况下使用名为 password 和 publickey 两种认证方式。

在全局配置态下使用下面的命令配置认证方式：

命令	目的
ip sshd auth-method	配置认证方式。

4.2.4 配置静默时间

ssh server 缺省情况下使用的静默时间为 60 秒，连续认证 6 次失败后，在一段时间（即静默时间）内禁止 ssh 登陆。

在全局配置态下使用下面的命令配置静默时间：

命令	目的
ip sshd auth-method *0-3600*	配置静默时间。

4.2.5 配置 aes

ssh server 缺省情况下是禁止 aes 加密方式功能的。

在全局配置态下使用下面的命令配置禁止 aes 加密方式：

命令	目的
ip sshd disable-aes	配置禁止aes加密方式

4.2.6 配置最大用户数

ssh server 缺省情况下是支持 10 个用户数。

在全局配置态下使用下面的命令配置 ssh 的最大用户数：

命令	目的
ip sshd max-user *1-16*	配置ssh最大用户数

4.2.7 配置文件下载功能

ssh server 缺省情况下是不支持文件下载功能。

在全局配置态下使用下面的命令使能 ssh 的文件下载功能：

命令	目的

ip sshd sftp-enable	使能ssh的文件下载功能

4.2.8 配置压缩功能

ssh server 缺省情况下是不支持压缩功能。使能后支持 zlib 压缩。

在全局配置态下使用下面的命令使能 ssh 的压缩功能：

命令	目的
ip sshd compress-enable	使能ssh的压缩功能

4.2.9 配置压缩等级

ssh server 缺省情况下的压缩等级是 6。数字越大压缩比就越大。

在全局配置态下使用下面的命令配置 ssh 的压缩等级：

命令	目的
ip sshd compress-level *0-9*	配置ssh的压缩等级

4.2.10 配置访问列表

为了控制对设备的 ssh server 的访问，可以为 ssh server 配置访问控制列表。

在全局配置态下使用下面的命令配置访问控制列表：

命令	目的
Ip sshd access-class STRING	配置访问控制列表

4.2.11 配置认证超时时长

客户端和 server 建立连接之后，如果不能在设置的时间之内通过认证，server 将关闭连接。

在全局配置态下使用下面的命令配置访问控制列表：

命令	目的
Ip sshd timeout <60-65535>	配置认证超时时长。

4.2.12 配置认证重试次数

当用户认证失败超过最大次数后，除非重新发起连接，否则 SSH server 不允许用户继续尝试，缺省情况下允许重试 3 次。

在全局配置态下使用下面的命令配置最大重试次数：

命令	目的
Ip sshd auth-retries <0-65535>	配置最大认证重试次数。

4.2.13 使能 ssh server

缺省条件下 SSH server 是关闭的，使能 SSH server 时，设备会生成一个 rsa 密钥对，并随后监听来自 client 的连接请求。这个过程大概需要一到两分钟的时间。

在全局配置态下使用下面的命令使能 SSH server：

命令	目的
Ip sshd enable	使能ssh server，密钥的位数为1024。

4.3 Ssh server配置示例

下面的配置只允许 IP 为 192.168.20.40 的主机访问 ssh server，使用本地用户数据库鉴别用户身份。

4.3.1 访问控制列表

```
ip access-list standard ssh-acl
permit 192.168.20.40
```

4.3.2 全局配置

```
aaa authentication login ssh-auth local
ip sshd pwd-method authentication-list  ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```