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 文件系统的管理 1
1.1.2 文件系统命令 1
1.1.3 手工从某一文件中启动 1
1.1.4 软件更新 2
1.1.5 配置更新 3
1.1.6 使用ftp进行软件和配置的更新 3
1.2 基本系统管理配置 4
1.2.1 配置以太网IP地址 4
1.2.2 配置缺省路由 5
1.2.3 利用PING测试网络连通状态 5
1.3 HTTP配置 5
1.3.1 HTTP配置 5
1.3.2 http配置示例 6
第 2 章 配置终端 8
2.1 VTY配置概述 8
2.2 配置任务 8
2.2.1 线路和接口之间的关系 8
2.3 监视与维护 8
2.4 VTY配置举例 9
第 3 章 网络管理配置 10
3.1 配置SNMP 10
3.1.1 概述 10
3.1.2 SNMP配置任务 11
3.1.3 配置实例 14
3.2 配置RMON 14
3.2.1 RMON配置任务 14
3.3 配置PDP 18
3.3.1 概述 18
3.3.2 PDP配置任务 18
3.3.3 PDP配置实例 19
第 4 章 Ssh 配置命令 21
4.1 SSH概述 21
4.1.1 SSH server 21
4.1.2 SSH client 21

4.1.3 实现特性 21
4.2 配置任务 21
4.2.1 配置认证方法列表 21
4.2.2 配置访问列表 21
4.2.3 配置认证超时时长 22
4.2.4 配置认证重试次数 22
4.2.5 使能ssh server 22
4.3 Ssh server配置示例 22
4.3.1 访问控制列表 22
4.3.2 全局配置 22

第1章　系统管理配置

1.1　配置文件管理

1.1.1　文件系统的管理

FLASH 中文件的名字最长只能有 20 个字符，且不区分大小写。

1.1.2　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。

命令	目的
format	格式化文件系统，删除所有数据。
dir [filename]	显示文件和目录名。[]内文件名是指显示以某几个字母开头的文件。文件显示的格式如下： 索引号　文件名　〈FILE〉　文件长度　　创立时间
delete　filename	删除一个文件，如果文件不存在，提示该文件不存在。
md　dirname	建立一个目录。
rd dirname	删除一个目录，如果目录不存在，提示该目录不存在。
more filename	显示一个文件的内容，如果文件内容多于一屏，将会自动分页显示。
cd	更改当前文件系统路径。
pwd	显示当前的路径。

1.1.3　手工从某一文件中启动

monitor#boot flash <*local_filename*>

本命令是用来启动闪存中的某个交换机软件，闪存中可能存有多个交换机软件.

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 switch.bin

1.1.4 软件更新

用户可使用本命令从本地或远程下载交换机系统软件， 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 flash [ip_addr]

本命令是用来从 tftp 服务器拷贝文件到系统的闪存，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
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，写入交换机叫“switch. bin”

monitor#copy tftp flash

提示：Source file name[]?main.bin

提示：Remote-server ip address[]?192.168.20.1

提示：Destination file name[main.bin]?switch.bin

please wait ...
##
##
##
##
##
##
TFTP:successfully receive 3377 blocks ,1728902 bytes
monitor#

1.1.5 配置更新

交换机的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

1.1.6 使用ftp进行软件和配置的更新

config #copy ftp flash [ip_addr|option]

在正式程序中管理态还可以使用 ftp 进行软件和配置的更新。使用 **copy** 命令可以从 **ftp** 服务器下载文件到交换机，也可以将交换机文件系统中的某个文件上载到 ftp 服务器。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。

copy{**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}|**flash**:filename>}{**flash**<:filename>|**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}<blksize><mode><type>

参数说明

参数	参数说明
login-nam	ftp 服务器的用户名。若没有指定，copy命令执行后将提示用户输入。
login-password	ftp 服务器的用户口令。若没有指定，copy命令执行后将提示用户输入。
nchecksize	在服务器上不检测文件大小
vrf	对支持MPLS的设备提供vrf绑定功能
blksize	数据传输块大小（缺省值512）
ip_addr	ftp 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。
active	指定以主动方式连接ftp server
passive	指定以被动方式连接ftp server
type	设置传输数据类型（以ascii方式还是Binary 方式）

举例

从服务器下载“main.bin”的文件，写入交换机叫“switch. bin”。

config#copy ftp flash

提示：ftp user name[anonymous]? login-nam

提示：ftp user password[anonymous]? login-password

提示：Source file name[]?main.bin

提示：Remote-server ip address[]?192.168.20.1

提示：Destination file name[main.bin]?switch.bin

或

config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin
##
##
FTP:successfully receive 3377 blocks ,1728902 bytes
config#

注：

1) 当 ftp server 无法访问，等待时间较长，由于 tcp 超时时间造成的（默认为 75s），可以通过设置全局命令 ip tcp synwait-time 修改 tcp 连接时间，但不建议使用。

2) 使用 ftp 时需要在某些网络状况下可能存在数据传输较慢情况，此时请适当调整传输块大小以取得最好效果。默认大小为 512 字节，可以在绝大多数网络中取得较高的运行效率。

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 192.168.20.100
PING 192.168.20.100: 56 data bytes
64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms
----192.168.20.100 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

1.3 HTTP配置

1.3.1 HTTP配置

- 使能 http 服务
- 改变 http 服务的端口号

- 配置 http 服务的访问口令
- 为 http 服务指定访问控制列表

1. 使能http服务

默认情况下 http 服务是关闭的。

在全局配置态下使用下面的命令使能 http 服务：

命令	目的
Ip http server	使能http 服务

2. 改变http服务的端口号

默认情况下 http 服务的监听端口是 80。

在全局配置态下使用下面的命令进行改变 http 服务的端口号：

命令	目的
Ip http port number	改变http服务的端口号

3. 配置http服务的访问口令

http 使用 enable 口令作为访问口令，如果要对 http 访问进行认证需要设置 enable 口令，在全局配置态下使用下面的命令可以配置 enable 口令：

命令	目的
Enable password {0|7} line	配置enable口令。

4. 为http服务指定访问控制列表

为了控制主机对 http 服务的访问，可以为 http 服务指定访问控制列表，在全局配置态下使用下面的命令可以为 http 服务指定访问控制列表。

命令	目的
ip http access-class STRING	为http服务指定访问控制列表。

1.3.2 http配置示例

下面的示例使用默认端口（80）作为 http 的服务端口，并限制只允许从 192.168.20.0/24 访问；

- ip acl 配置：

  ip access-list standard http-acl

  permit 192.168.20.0 255.255.255.0

- 全局配置：

  ip http access-class http-acl

  ip http server

第2章　配置终端

2.1　VTY配置概述

系统使用 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

系统有四种类型的线路：控制台，辅助，异步和虚拟终端线路。不同系统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	用于登录到系统进行配置服务。	编号0。
VTY	虚拟异步	用于连接到系统上的同步端口[如以太网和串行接口]的 Telnet,X.25 PAD、HTTP和Rlogin等。	从一开始的32个编号。

2.2.1　线路和接口之间的关系

1. 同步接口和VTY线路间关系

虚拟终端线路提供了通过同步接口对系统进行的访问。当一个用户通过 VTY 线路连接到系统时，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：

(1)　进入行配置模式。

(2)　对终端参数配置。

可以参见后面的“VTY 配置举例”部分，了解 VTY 的配置。

2.3　监视与维护

用 show line 命令查看 VTY 的配置。

2.4 VTY配置举例

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 32
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 驻留在系统上。配置系统上的 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、与邻近系统连接的丢失或其它重要的事件。

1. SNMP 通告

特殊事件发生时系统能向 SNMP 管理端发送通知(inform)。例如，当代理系统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，所以它们消耗了系统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系统的内存，并且不必收到每个通知，可使用陷阱。

本公司系统目前支持陷阱，但提供了对通知请求的扩充。

2. SNMP的版本

本公司系统现支持下面的 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。

本公司三层交换机还支持下面版本的 SNMP：

- SNMPv3--- 简单网络管理协议版本 3，在 RFC3410 中定义。

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。

SNMPv3 通过对 SNMP 报文进行认证和加密操作来提供对设备访问的安全性。

SNMPv3 提供了下列安全特性：

- 消息完整性：保证消息在传输过程中没有被篡改
- 认证：确保消息的来源地的合法性
- 加密：对消息题进行加密，未经认证的主机即使窃取到消息也无法解密阅读

SNMPv3 提供安全模型和安全级别。安全模型是指一种认证策略，通过配置用户名和该用户所属的组来实现。安全级别是指安全模型中支持的不同的认证方式。SNMPv3 基于用户的安全模型支持三种安全级别，按照从高到低的顺序排列分别是认证并加密、认证不加密和不认证；通过使用 MD5 或 SHA 散列算法计算认证密钥的摘要值在网络间传送并在 SNMP 引擎比对来实现密码不被泄漏，使用 DES 加密算法对报文进行加密保证设备不被第三者窃听。通过配置用户/密码对和用户所属的组来实现管理者对设备的身份认证，通过配置组和视图决定组内的用户不同操作对于管理信息库的访问权限；组同时限制了组内用户的最低安全级别。

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

本公司系统的 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)。

本公司系统为每个系统提供了自己私有的 MIB 扩充。

3.1.2 SNMP配置任务

SNMP 配置任务有：

- 配置 SNMP 视图

- 为 SNMP 团体创建或修改访问控制
- 设置该系统管理员的联系方法和系统所在位置
- 定义 SNMP 代理数据包的最大长度
- 监视 SNMP 状态
- 配置 SNMP 陷阱

1. 配置SNMP视图

SNMP 视图用于规定管理信息库的访问权限：允许访问和拒绝访问。使用下面的命令配置 SNMP 视图

命令	说明
snmp-server view *name oid*] [exclude | include]	将oid指定的管理信息库叶子或表加入SNMP视图name中，并指定SNMP视图name中oid指定的对象标示符的访问权限，exclude为拒绝访问，include为允许访问

SNMP 视图中可以访问的子集为所有配置了允许访问的管理信息库的对象除去所有配置了拒绝访问的对象；未配置的对象默认权限为不可访问。

配置了 SNMP 视图后，可以将 SNMP 视图应用到 SNMP 团体名的配置中，用以限定该团体名的可访问对象的子集。

2. 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系统上代理的口令。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。

关于配置团体字符串的示例，参见"SNMP 命令”一章。

3. 设置该系统管理员的联系方法和系统所在位置

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（系统）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。

4. 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。

5. 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。

6. 配置SNMP陷阱

使用下面的命令配置系统发送 SNMP 陷阱（第二个任务是可选的）：

- 配置系统发送陷阱

  在全局配置模式下使用下面的命令配置系统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。

系统开机后，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，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。

7. SNMP绑定源地址

在全局配置模式下使用下面的命令，设置 SNMP 报文的源地址功能。

命令	目的
snmp source-addr *ipaddress*	设置SNMP报文的源地址

3.1.3 配置实例

1. 例一

```
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 读系统中 MIB 变量，用 private 读系统中的 MIB 变量与写系统中可写的 MIB 变量。它还指定了当系统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。例如当系统的某个端口 down 时，系统会向 192.168.20.2 发送一条 linkdown 的陷阱消息。

3.2 配置RMON

3.2.1 RMON配置任务

RMON 配置任务有：

- 配置交换机 rMon 告警功能
- 配置交换机 rMon 事件功能
- 配置交换机 rMon 统计功能
- 配置交换机 rMon 历史功能
- 显示交换机 rMon 配置

1. 配置交换机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，还需要对交换机的 SNMP 进行配置。告警功能配置完成后，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* [*eventnumber*] [**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. 配置交换机rMon事件功能

配置 rMon 事件步骤如下：

步骤	命令	目的
1.	**configure**	进入全局配置模式。
2.	**rmon event index** [**description** *string*] [**log**] [**owner** *string*] [**trap** community]	增加一个rMon事件表项。 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。
3.	**exit**	退回到管理模式。
4.	**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. 配置交换机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：

步骤	命令	目的
1.	**configure**	进入全局配置模式。
2.	**interface iftype ifid**	进入端口模式。 iftype为端口的类型 。 ifid为接口的id。
3.	**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。
4.	**exit**	退回到全局模式 。
5.	**exit**	退回到管理模式 。
6.	**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. 配置交换机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：

步骤	命令	目的
1.	configure	进入全局配置模式
2.	interface iftype ifid	进入端口模式 iftype为端口的类型 ifid为接口的id
3.	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
4.	exit	退回到全局模式
5.	exit	退回到管理模式
6.	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. 显示交换机RMON配置

使用 show 命令显示交换机 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。

本公司交换机上的 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，交换机只能处于网络边缘，否则，将不能获得完整的网络拓扑结构。

交换机上的 PDP 能够配置于所有的 SANP 上（如以太网等）。

3.3.2 PDP配置任务

- 交换机 PDP 默认配置
- 设置 PDP 时钟和信息保存时间
- 设置 PDP 的版本
- 启动交换机上的 PDP
- 启动交换机端口上的 PDP
- 监控和管理 PDP

1. 交换机PDP默认配置

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。
PDP版本	2。

2. 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。

3. 设置PDP的版本

设置 PDP 支持的版本时，可以在全局配置模式下使用下面的命令：

命令	目的
pdp version {1|2}	配置PDP的版本。

4. 启动交换机上的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	启动交换机上的PDP功能。

5. 启动交换机端口上的PDP

PDP 在默认配置下是没有启动的，当启动交换机上的 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	启动交换机端口上的PDP功能。

6. 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	显示交换机接收和发送的PDP报文计数。
show pdp neighbor [detail]	显示交换机通过PDP发现的邻居。

3.3.3 PDP配置实例

例 1：启动 PDP 功能。

config# pdp run
config# int f0/0
config_f0/0#pdp enable

例 2：配置 PDP 时钟和信息保存时间。

config#**pdp timer** 30
config#**pdp holdtime** 90

例 3：配置 PDP 的版本。

config#pdp version 1

例 4：监控 PDP 信息。

config#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 配置命令

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。

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。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 auth_method STRING	配置认证方法列表。

4.2.2 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

4.2.3 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。

4.2.4 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。

4.2.5 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 auth-method ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```