基础配置

目 录

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 | cf} <*local_filename*>

本命令是用来启动闪存或 CF 卡中的某个交换机软件，闪存或 CF 卡中可能存有多个交换机软件。

参数说明

参数	参数说明
flash	文件存储在flash闪存中
cf	文件存储在CF卡中

local_filename	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，从而获得版本升级，或获得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，采用如下文所述方式更新软件。

1. 通过 TFTP 协议

monitor#copy tftp {flash: | cf:} [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

参数或关键字	参数说明
flash:	存储设备为flash闪存
cf:	存储设备为CF卡
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在 flash 上，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

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

参数说明

参数	参数说明
login-name	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
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”。

switch#copy ftp flash

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

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

switch#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

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0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：

```
Switch_config# line vty 0 31
Switch_config_line# length 0
```

第 3 章　SSH 配置命令

3.1　SSH概述

3.1.1　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。

3.1.2　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。

3.1.3　实现特性

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

3.2　配置任务

3.2.1　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。认证方法名的长度不超过20个字符。

3.2.2　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。访问控制列表名的长度不超过19个字符。

3.2.3 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认证超时时长：

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

3.2.4 配置认证重试次数

当用户认证失败超过最大次数后，将暂时关闭 ssh server 服务，进入登录静默期。缺省情况下允许重试 6 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。

3.2.5 配置登录静默期时长

当累计登录认证失败次数超过设置阀值时，将进入登录静默期，缺省情况下，静默期时长为 60s。

在全局配置态下使用下面的命令配置登录静默期时长：

命令	目的
ip sshd silence-period <0-3600>	配置登录静默期时长。

3.2.6 使能 sftp 功能

sftp 功能是指基于 ssh 协议的安全文件传输系统，其认证过程以及数据传输均被加密保护，传输效率较低，但网络安全性大为提高。

缺省条件下 sftp 功能是关闭的，在全局配置态下使用下面的命令使能 sftp 功能：

命令	目的
ip sshd sftp	使能sftp功能

3.2.7 使能密钥保存功能

使能 ssh server 时需要计算初始密钥 ，这个过程可能需要一到两分钟的时间。开启密钥保存功能之后，初始密钥会被保存到 flash 中，当再次启动 ssh server 时，首先从 flash 中读取密钥，避免重复计算，缩短启动时间。

缺省条件下密钥保存功能是关闭的，在全局配置态下使用下面的命令使能密钥保存功能：

命令	目的
ip sshd save	使能密钥保存功能

3.2.8 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。

3.3 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。

3.3.1 访问控制列表

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

3.3.2 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
```