# Basic Configuration

# Table of Contents

# Chapter 1 **System Management Configuration**

## 1.1 File Management Configuration

### 1.1.1 Managing the file system

The filename in flash is no more than 20 characters and filenames are case insensitive.

### 1.1.2 Commands for the file system

The boldfaces in all commands are keywords. Others are parameters. The content in the square brakcet “[ ]” is optional.

| Command | Description |
|---|---|
| **format** | Formats the file system and delete all data. |
| **dir** [filename] | Displays files and directory names. The file name in the symbol “[]” means to display files starting with several letters. The file is displayed in the following format:<br>Index number file name <FILE> length established time |
| **delete** filename | Deletes a file. The system will prompt if the file does not exist. |
| md dirname | Creates a directory. |
| rd dirname | Deletes a directory. The system will prompt if the directory is not existed. |
| more filename | Displays the content of a file. If the file content cannot be displayed by one page, it will be displayed by pages. |
| cd | Changes the path of the current file system. |
| pwd | Displays the current path. |

### 1.1.3 Starting up from a file manually

monitor#boot flash <*local_filename*>

The previous command is to start a switch software in the flash, which may contain multiple switch software.

Parameter

| Parameter | Description |
|---|---|
| Flash | A file stored in the flash memory. |
| *local_filename* | A file name stored in the flash memory<br>Users must enter the file name. |

Example

monitor#boot flash switch.bin

### 1.1.4 Updating software

User can use this command to download switch system software locally or remotely to obtain version update or the custom-made function version (like data encryption and so on).

There are two ways of software update in monitor mode.

1. Through TFTP

monitor#copy tftp flash: [ip_addr]

The previous commad is to copy file from the tftp server to the flash in the system. After you enter the command, the system will prompt you to enter the remote server name and the remote filename.

Parameter

| Parameter | Description |
|---|---|
| flash | Store device in the flash memory. |
| ip_addr | IP address of the tftp server<br>If there is no specified IP address, the system will prompt you to enter the IP address after the **copy** command is run. |

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin**.

monitor#copy tftp flash

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

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

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

### 1.1.5 Updating configuration

The switch configuration is saved as a file, the filename is startup-config. You can use commands similar to software update to update the configuration.

1. Through TFTP

monitor#copy tftp flash startup-config

### 1.1.6 Using ftp to perform the update of software and configuration

switch #copy ftp {flash|cf} [ip_addr|option]

Use ftp to perform the update of software and configuration in formal program management. Use the **copy** command to download a file from ftp server to switch, also to upload a file from file system of the switch to ftp server. After you enter the command, the system will prompt you to enter the remote server name and remote filename.

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

Parameter

| Parameter | Description |
|---|---|
| login-nam | Username of the ftp server<br>If there is no specified username, the system will prompt you to enter the username after the **copy** command is run. |
| login-password | Password of the ftp server<br>If there is no specified password, the system will prompt you to enter the password after the **copy** command is run. |
| nchecksize | The size of the file is not checked on the server. |
| blksize | Size of the data transmission block<br>Default value: 512 |
| ip_addr | IP address of the ftp server<br>If there is no specified IP address, the system will prompt you to enter the IP address after executing the **copy** command. |
| active | Means to connect the ftp server in active mode. |
| passive | Means to connect the ftp server in passive mode. |
| type | Set the data transmission mode (ascii or binary) |

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin**.

config#copy ftp flash

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

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

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

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

or

config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin
##########################################################################
##########################################################################

FTP:successfully receive 3377 blocks ,1728902 bytes
config#

**Note:**

1) When the ftp server is out of service, the wait time is long. If this problem is caused by the tcp timeout time (the default value is 75s), you can configure the global command **ip tcp synwait-time** to modify the tcp connection time. However, it is not recommended to use it.

2) When you use ftp in some networking conditions, the rate of data transmission might be relatively slow. You can properly adjust the size of the transmission block to obtain the best effect. The default size is 512 characters, which guarantee a relatively high operation rate in most of the networks.

## 1.2 Basic System Management Configuration

### 1.2.1 Configuring Ethernet IP address

monitor#ip address <*ip_addr*> <*net_mask*>

This command is to configure the IP address of the Ethernet. The default IP address is 192.168.0.1, and the network mask is 255.255.255.0.

Parameter

| Parameter | Description |
|---|---|
| *ip_addr* | IP address of the Ethernet |
| *net_mask* | Mask of the Ethernet |

Example

monitor#ip address 192.168.1.1 255.255.255.0

### 1.2.2 Configuring default route

monitor#ip route default <*ip_addr*>

This command is used to configure the default route. You can configure only one default route.

Parameter

| Parameter | Description |
|---|---|
| *ip_addr* | IP address of the gateway |

Example

monitor#ip route default 192.168.1.1

### 1.2.3 Using ping to test network connection state

monitor#ping <*ip_address*>

This command is to test network connection state.

Parameter

| Parameter | Description |
|---|---|
| *ip_address* | Destination IP address |

Example

```
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
```

# Chapter 2 **Terminal Configuration**

## 2.1 VTY Configuration Introduction

The system uses the **line** command to configure terminal parameters. Through the command, you can configure the width and height that the terminal displays.

## 2.2 Configuration Task

The system has four types of lines: console, aid, asynchronous and virtual terminal. Different systems have different numbers of lines of these types. Refer to the following software and hardware configuration guide for the proper configuration.

| Line Type | Interface | Description | Numbering |
|---|---|---|---|
| CON(CTY) | Console | To log in to the system for configuration. | 0 |
| VTY | Virtual and asynchronous | To connect Telnet, X.25 PAD, HTTP and Rlogin of synchronous ports (such as Ethernet and serial port) on the system | 32 numbers starting from 1 |

### 2.2.1 Relationship between line and interface

1. Relationship between synchronous interface and VTY line

The virtual terminal line provides a synchronous interface to access to the system. When you connect to the system through VTY line, you actually connects to a virtual port on an interface. For each synchronous interface, there can be many virtual ports.

For example, if several Telnets are connecting to an interface (Ethernet or serial interface), you need to do the following steps for the VTY configuration:

(1) Log in to the line configuration mode.

(2) Configure the terminal parameters.

For VTY configuration, refer to Part 2.4 “VTY configuration example”.

## 2.3 Monitor and Maintenance

Run **showline** to chek the VTY configuration.

## 2.4 VTY Configuration Example

It shows how to cancel the limit of the line number per screen for all VTYs without **more** prompt:

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

# CHAPTER 3 **SSH Configuration Commands**

## 3.1 Introduction

### 3.1.1 SSH server

A scure and encrypted communication connection can be created between SSH client and the device through SSH server. The connection has telnet-like functions. SSH server supports the encryption algorithms including des, 3des and blowfish.

### 3.1.2 SSH client

SSH client is an application running under the ssh protocol. SSH client can provide authentication and encryption, so SSH client gurantees secure communication between communication devices or devices supporting SSH server even if these devices run in unsafe network conditions. SSH client supports the encryption algorithms including des, 3des and blowfish.

### 3.1.3 Function

SSH server and SSH client supports version 1.5. Both of them only support the shell application.

## 3.2 Configuration Tasks

### 3.2.1 Configuring the authentication method list

SSH server adopts the login authentication mode. SSH server uses the **default** authentication method list by default.

Run the following command in global configuration command mode to configure the authentication method list:

| Command | Purpose |
|---|---|
| Ip sshd auth_method STRING | Configures the authentication method list.<br>The length of the authentication method name is no more than 20 characters. |

### 3.2.2 Configuring the access control list

To control the access to the device's SSH server, you need to configure the access control list for SSH server.

Run the following command in global configuration mode to configure the access control list:

| Command | Purpose |
|---|---|
| Ip sshd access-class STRING | Configures the access control list. The length of the access control list name is no more than 19 characters. |

### 3.2.3 Configuring the authentication timeout value

After a connection is established between client and server, server cuts off the connection if authentication cannot be approved within the set time.

Run the following command in global configuration mode to configure the configuration timeout value:

| Command | Purpose |
|---|---|
| Ip sshd timeout <60-65535> | Configures the authentication timeout value. |

### 3.2.4 Configuring the times of authentication retrying

If the times for failed authentications exeed the maximum times, SSH server will not allow you to retry authentication unless a new connction is established. The maximum times for retrying authentication is 6 by default.

Run the following command in global configuration mode to configure the maximum times for retrying authentication:

| Command | Purpose |
|---|---|
| Ip sshd auth-retries <0-65535> | Configures the maximum times for retrying authentication. |

### 3.2.5 Configuring the login silence period

When the failure login times exceed the threshold, the device enters the login silence period. The silence period is 60s.

Run the following command to configure the login silence period in the global configuration mode:

| Command | Purpose |
|---|---|
| ip sshd silence-period <0-3600> | Configures the login silence period. |

### 3.2.6 Enabling sftp

Stp is a security file transmission system based on the ssh protocol whose authentication and data transmission are encrypted. Though its transmition rate is slow, it has a strong network security.

Sftp is diabled by default. Run the following command to enable sftp in the global configuration mode:

| Command | Purpose |
|---|---|
| ip sshd sftp | Enables sftp. |

### 3.2.7 Enabling sshd

It takes one to two minutes to calculate the initial password when enabling ssh server. The initial password will be saved in **flash** when enabling the function. The device will read the encryption key from **flash** when reenabling ssh server. Thus, the start time is shortened.

The sshd (encryption key saving) is disabled by default. Run the following command to enable sshd (encryption key saving) in the global configuration mode:

| Command | Purpose |
|---|---|
| ip sshd save | Enables sshd |

### 3.2.8 Enabling SSH server

SSH server is disabled by default. When SSH server is enabled, the device will generate a rsa password pair, and then listen connection requests from the client. The process takes one or two minutes.

Run the following command in global configuration mode to enable SSH server:

| Command | Purpose |
|---|---|
| Ip sshd enable | Enables SSH server. The digit of the password is 1024. |

## 3.3 SSH server Configuration Example

The following configuration only allows the host whose IP address is 192.168.20.40 to access SSH server. The local user database is used to distinguish user ID.

### 3.3.1 Access control list

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

### 3.3.2 Global configuration

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