Chapter 2: 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	Purpose
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: 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 command is to start a switch software in the flash, which may contain multiple switch softwares.

Description

Parameters	Description
Flash	A file name stored in the flash memory
local_filename	file name, the user 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.

Through TFTP protocol

monitor#copy tftp flash: [ip_addr]

The command 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.

Description

parameters or keywords	Description
flash:	The memory device is flash memory.
ip_addr	Means the IP address of the TFTP server. If this parameter is not designated, you are prompted 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 protocol

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

Description

Parameters	Description
login-name	Username of the ftp server If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.
login-password	Password of the ftp server If this parameter is not designated, you are prompted to enter the IP address 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 (Default value: 512)
ip_addr	IP address of the ftp server If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.
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.

switch#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

switch#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.

Description

Parameters	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 Setting the default route.

monitor#ip route default <*ip_addr*>

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

Description

Parameters	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.

Description

Parameters	Description
ip_address	Stands for the 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 Overview

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 Tasks

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 0

2.2.1 Relationship between line and interface

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) (1) Log in to the line configuration mode.

(2) (2) Configure the terminal parameters.

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

2.3 Monitor and Maintenance

Run show line to check 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

2.5 SSH Overview

2.5.1 SSH server

SSH client can provide a secure and encrypted communication link throughSSH server and other devices. This connection has the same functions as those of Telnet. SSH server supports the following encryption algorithms: des, 3des and blowfish.

2.5.2 SSH client

SSH client runs on the basis of the SSH protocol, providing authentication and encryption. Due to the application of authentication and encryption,SSH client allows to establish secure communication in unsecure network environment between communication devices or between other devices that supportSSH server. SSH client supports the following encryption algorithms: des, 3des and blowfish.

2.5.3 Attribute Realization

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

2.6 Configuration Tasks

2.6.1 Configuring the Authentication Method List

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

In global configuration mode, the following command can be used to configure the authentication method list.

Command	Purpose
ip sshd auth-method STRING	Configure the authentication method list. The length of the authentication method's name is no more than 20 characters.

2.6.2 Configuring Access List

In order to control SSH server to access other devices, you can configure ACL for SSH server.

In global configuration mode, the following command can be used to configure the timeout time.

Command	Purpose
ip sshd access-class STRING	Configure ACL. The length of the access list's name is no more than 19 characters.

2.6.3 Configuring the Authentication Timeout Time

After SSH client connects SSH server successfully, the SSH server will close the connection if the authentication cannot be passed during the configured time.

In global configuration mode, the following command can be used to configure the authentication timeout.

Command	Purpose
ip sshd timeout <60-65535>	Configure the authentication timeout time.

2.6.4 Configuring the Authentication Retry Times

If the times for failed authentications exceed the maximum times, SSH server will not allow you to retry authentication and the system enters the silent period. The maximum times for retrying authentication is 6 by default.

In global configuration mode, the following command can be used to configure the authentication retry times.

Command	Purpose
ip sshd auth-retries <0-65535>	Configure the authentication retry times.

2.6.5 Configuring the Login Silence Period

The system enters in the silent period when the authentication retry times exceed the threshold. The silence period is 60s by default.

In global configuration mode, the following command can be used to configure the silence period.

Command	Purpose
ip sshd silence-period <0-3600>	Configuring the login silence period

2.6.6 Enabling SFTP

The SFTP function refers to the secure file transmission system based on SSH, of which the authentication procedure and data transmission are encrypted. Though it has low transmission efficiency, network security is highly improved.

SftpFUNCTIONis disabled by default. Run following command to enable sftpFUNCTIONin global configuration mode.

Command	Purpose
ip sshd sftp	Enable sftp function.

2.6.7 Enabling Encryption Key Saving Function

Enable ssh server and the initial encryption key needs to be calculated. The process may take one to two minutes. When enabling the encryption key saving function, the initial encryption key is saved in the flash. When enabling ssh server in a second time, the encryption key will be read first.

sftp function is disabled by default.USE THE FOLLOWING COMMANDto enable sftpFUNCTION IN GLOBAL CONFIGURATION MODE:

Command	Purpose
ip sshd save	Enable encryption key saving function.

2.6.8 Enabling SSH Server

SSH server is disabled by default. WhenSSH server is enabled, a RSA key pair will be generated and then listens the connection request from SSH client. The whole process probably requires one or two minutes.

The following command can be used in global configuration mode to enableSSH server **:**

Command	Purpose
ip sshd enable	Enable SSH server. The digit of the password is 1024.

2.7 Configuration Example of SSH Server

The following configuration allows the host whose IP is 192.168.20.40 to access SSH server, while the local user database will be used to authenticate the user.

2.7.1 ACL

ip access-list standard ssh-acl

permit 192.168.20.40

2.7.2 Global Configuration

aaa authentication login ssh-auth local

ip sshd auth-method ssh-auth ip sshd

access-class ssh-acl ip sshd enable