FiberstoreOS
Basic Configuration Guide

Contents

1 Configuring System Management

1.1 Overview

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner displays on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner also displays on all connected terminals. It appears after the MOTD banner and before the login prompts.

1.2 Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the switch.

To enable message logging, follow these steps:

Switch# configure terminal	Enter global configuration mode
Switch(config)# banner motd c message c	Specify the message of the day. For c, enter the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For message, enter a banner message up to 255 characters. You cannot use the delimiting character in the message
Switch(config)# exit	Exit the Configure mode

1.3 Configuring a Login Banner

You can configure a login banner to be displayed on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Beginning in privileged EXEC mode, follow these steps to configure a login banner:

Switch# configure terminal	Enter global configuration mode
Switch(config)# banner login c message c	Specify the login message. For c, enter the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For message, enter a login message up to 255 characters. You cannot use the delimiting character in the message
Switch(config)# exit	Exit the Configure mode

1.4 Configuring an Exec Banner

You can configure an exec banner to be displayed on all connected terminals. This banner appears when terminal in privileged EXEC mode.

Beginning in privileged EXEC mode, follow these steps to configure an exec banner:

Switch# configure terminal	Enter global configuration mode
Switch(config)# banner exec c message c	Specify the login message. For c, enter the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For message, enter a login message up to 255 characters. You cannot use the delimiting character in the message
Switch(config)# exit	Exit the Configure mode

1.5 Validation Commands

All current banner configurations can be displayed. To display, follow these steps:

Switch# show running	Show the current system configuration

2 Configuring User Management

2.1 Overview

User management increases the security of the system by keeping the unauthorized users from guessing the password. The user is limited to a specific number of attempts to successfully log in to the switch.

There are three load modes in the switch. In “no login” mode, anyone can load the switch without authentication. In “login” mode, there is only one default user. In “login local” mode, if you want to load the switch you need to have a user account.

Local user authentication uses local user accounts and passwords that you create to validate the login attempts of local users. Each switch has a maximum of 32 local user accounts. Before you can enable local user authentication, you must define at least one local user account.

You can set up local user accounts by creating a unique username and password combination for each local user. Each username must be fewer than 32 characters.

You can configure each local user account with a privilege level; the valid privilege levels are 1 or 4. Once a local user is logged in, only the commands those are available for that privilege level can be displayed.

2.2 Configuring the user management in login local mode

2.2.1 Configurations

Switch# configure terminal	Enter global configuration mode
Switch(config)# line vty 0 7	Enter line configuration mode, use line console 0 if you want to set console port access

Switch(config-line)# login local	Enable local login authentication on the switch
Switch(config-line)# exit	Enter global configuration mode
Switch(config)#username testname privilege 4 password 123abc<>	Create a local user account
Switch(config)# exit	Exit the global configure mode

2.2.2 Validation Command

After the above setting, login the switch will need a username and password, and user can login with the username and password created before. This is a sample output of the login prompt.

```
Username: testname
Password:
```

2.3 Configuring the user management in login mode

The login mode requires the line password without a username.

2.3.1 Configurations

Switch# configure terminal	Enter global configuration mode
Switch(config)# line vty 0 7	Enter line configuration mode, use line console 0 if you want to set console port access
Switch(config-line)# login	Enable login authentication on the switch
Switch(config-line)# line-password abc	Set login password of abc
Switch(config-line)# end	Enter the Exec mode

2.3.2 Validation Command

After the above setting, login the switch will need the line password, and user can login with the password created before. This is a sample output of the login prompt.

```
Password:
```

2.4 Configuring Password recovery procedure

2.4.1 Configurations

If the password is forgotten unfortunately, it can be recovered by following steps.

Step 1 Power on the system. Boot loader will start to run. The follow information will be printed on Console.

```
CPU:   MPC8247 (HiP7 Rev 14, Mask 1.0 1K50M) at 350 MHz
Board: 8247 (PCI Agent Mode)
I2C:   ready
DRAM:  256 MB
In:    serial
Out:   serial
Err:   serial
Net:   FCC1 ETHERNET, FCC2 ETHERNET [PRIME]
Press ctrl+b to stop autoboot: 3
```

Step 2 Press ctrl+b. stop autoboot.

Step 3 Under boot loader interface, use the following instructions.

Bootrom# boot_flash_nopass	Load the device without start-config file under the boot loader mode through Console
Bootrom# Do you want to revert to the default config file ? [Y|N|E]:	Input “Y”

Then system will reboot without loading startup-configuration. No password will be required.

3 Configuring FTP

3.1 Overview

You can download a switch configuration file from an FTP server or upload the file from the switch to an FTP server. You download a switch configuration file from a server to upgrade the switch configuration. You can overwrite the current startup configuration file with the new one. You upload a switch configuration file to a server for backup purposes. You can use this uploaded configuration for future downloads to the switch or another switch of the same type.

3.2 IPv4 Configurations

3.2.1 Preparing to download or upload a configuration file by using FTP

You can copy configurations files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server.

Before you begin downloading or uploading a configuration file by using FTP, do these tasks:

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same network if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the ping command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download.
- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

3.2.2 Downloading a configuration file by using FTP

You can download a new configuration file and overwrite the current configuration or keep the current configuration.

Switch# configure terminal	Enter global configuration mode
Switch(config)# ftp username test	(Optional) Create a user “test”
Switch(config)# ftp password test	(Optional) Create a password “test”
Switch(config)# end	Return to privileged EXEC mode
Switch#copy mgmt-if ftp://test:test@10.10.10.163/ startup-config.conf flash:/startup-config.conf	Get a startup configuration file from remote FTP server. User’s name is “test”; the password is “test”
Switch# show startup-config	Verify your entries

3.2.3 Uploading a configuration file by using FTP

You can upload a configuration file from the switch to an FTP server. You can later download this configuration to the same switch or to another switch of the same type.

Beginning in privileged EXEC mode, follow these steps to upload a configuration file to an FTP server:

Switch# configure terminal	Enter global configuration mode
Switch(config)# ftp username test	(Optional) Create a user “test”
Switch(config)# ftp password test	(Optional) Create a password “test”
Switch(config)# end	Return to privileged EXEC mode
Switch# copy flash:/startup-config.conf mgmt-if ftp://test:test@10.10.10.163/startup-config.conf	Upload a startup configuration file to remote FTP server User’s name is “test”; the password is “test”

3.3 IPv6 Configurations

3.3.1 Downloading a configuration file by using FTP

Switch1

Switch# copy ftp://root:root@2001:1000::2/startup-config.conf flash:/startup-config.conf	Get a startup configuration file from remote FTP server. User's name is "root"; the password is "root"
Switch# show startup-config	Verify your entries

3.3.2 Uploading a configuration file by using FTP

Switch1

Switch# copy flash:/startup-config.conf mgmt-if ftp://root:root@2001:1000::2 startup-config.conf	Upload a startup configuration file to remote FTP server User's name is "root"; the password is "root"

4 Configuring TFTP

4.1 Overview

You can download a switch configuration file from a TFTP server or upload the file from the switch to a TFTP server. You download a switch configuration file from a server to upgrade the switch configuration. You can overwrite the current file with the new one. You upload a switch configuration file to a server for backup purposes; this uploaded file can be used for future downloads to the same or another switch of the same type.

4.2 Configurations

4.2.1 Preparing to download or upload a configuration file by using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured.
- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same network if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the ping command.
- Ensure that the configuration to be downloaded is in the correct directory on the TFTP server.
- For download operations, ensure that the permissions on the file are set correctly.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly.

4.2.2 Downloading a configuration file by using TFTP

You can download a new configuration file and replace the current file or keep the current file.

Switch# copy mgmt-if tftp://10.10.10.163/startup-config.conf flash:/startup-config.conf	Get a new configuration file from remote TFTP server
Switch# copy mgmt-if tftp://2001:1000::2/startup-config.conf flash:/startup-config.conf	Get a new configuration file from remote TFTP server
Switch# show startup-config	Verify your entries

4.2.3 Uploading a configuration file by using TFTP

You can upload a configuration file from the switch to a TFTP server. You can later download this file to the switch or to another switch of the same type.

Beginning in privileged EXEC mode, follow these steps to upload a configuration file to a TFTP server.

Switch# copy flash:/startup-config.conf mgmt-if tftp://10.10.10.163/startup-config.conf	Upload the startup configuration file to remote TFTP server
Switch# copy flash:/startup-config.conf mgmt-if tftp://2001:1000::2/startup-config.conf	Upload the startup configuration file to remote TFTP server

5 Configuring Telnet

5.1 Overview

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards.

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration (including systems based on Windows NT). Because of security issues with Telnet, its use for this purpose has waned in favor of SSH.

5.2 Configurations

Telnet switch with inner port.

Switch# telnet 10.10.29.247	Telnet switch 10.10.29.247 with inner port
Switch# telnet 2001:1000::71	Telnet switch 2001:1000::71 with inner port

Telnet switch with management port.

Switch# telnet mgmt-if 10.10.29.247	Telnet switch 10.10.29.247 with management port
Switch# telnet mgmt-if 2001:1000::2	Telnet switch 2001:1000::2 with management port

The switch also support telnet server.

Switch# configure terminal	Enter the Configure mode
Switch(config)# service telnet enable	Enable telnet service

5.3 Validation Commands

Switch# telnet mgmt-if 10.10.38.1

```
Entering character mode
Escape character is '^]'.
```

```
Switch #
```

Switch# telnet 2001:1000::71

```
Entering character mode
Escape character is '^]'.
```

Switch #

6 Configuring SSH

6.1 Overview

The Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication. The SSH feature has an SSH server and an SSH integrated client, which are applications that run on the switch. You can use an SSH client to connect to a switch running the SSH server. The SSH server works with the SSH client supported in this release and with SSH clients. The SSH client also works with the SSH server supported in this release and with SSH servers.

6.2 Topology

Figure 6-1 SSH system application

6.3 Configurations

Create key for SSH

Switch# configure terminal	Enter the Configure mode
Switch(config)# rsa key a generate	Create a key name a
Switch(config)# rsa key a export url flash:/a.pri private ssh2	Create a private key named a.pri with key a and save it to flash

Switch(config)# rsa key a export url flash:/a.pub public ssh2	Create a private key named a.pub with key a and save it to flash

Import the key

Switch(config)# rsa key importKey import url flash:/a.pub public ssh2	Import the key a.pub we created as importKey
Switch(config)#)# username aaa privilege 4 password abc	Create a user with name aaa.
Switch(config)# username aaa assign rsa key importKey	Assign the key to use aaa

6.4 Validation commands

On SSH client:

- Download the a.pri key
- load the switch

[root@test1 tftpboot]# ssh -i a.pri aaa@10.10.39.101

```
aaa@10.10.39.101's password:

Switch#
```

7 Configuring Time&timezone

7.1 Overview

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

7.2 Configurations

Switch# configure terminal	Enter into configure mode
Switch(config)# clock set datetime 11:30:00 10 26 2013	Set the current system time
Switch(config)# clock set summer-time dst date 6 1 2013 02:00:00 10 31 2013 02:00:00 120	Set the summer time
Switch(config)#exit	Exit from configure mode
Switch# show clock detail	Display the current time and date

7.3 Validation Commands

Switch# show clock detail

```
13:31:10 dst Sat Oct 26 2013
Time zone: (GMT + 08:00:00)  beijing
Summer time starts at beijing 02:00:00  06/01/2013
Summer time ends at dst 02:00:00  10/31/2013
Summer time offset:  120 minutes
```

8 Configuring License

8.1 Overview

License will control the features on the switch, Each switch has its own license to avoid the unauthorized user to use the advanced features. There are totally three kinds of licenses: Enterprise Base, Metro Service, and Metro Advanced. Different license will contain different features. Customer can apply different license to satisfy different requirement. If switch has no license, it can only provide L2 features.

Different switch can't share the same license. In order to get the license for the specify switch, first generate the unique device identifier(UDI) for the switch and then send the UDI to vendor to apply the license, at last get the license from vendor and use the license on the switch.

8.2 Configurations

Create UDI

Switch# generate device identifier mgmt-if ftp://test:test@10.10.25.33/device.udi	Create UDI for the device and send it to remote FTP server

Apply license

Send UDI file to vendor, vendor will generate license for customer requirement.

Use license

- You must reload the switch for the license to take effect.

- If the switch has no license, it can only work with L2 features.
- If the switch has more than one license, all the features contain by the licenses can take effect

Switch# copy mgmt-if ftp://test:test@10.10.25.33/device.lic flash:/device.lic	Get the license to local from remote FTP server
Switch# reload	Reload system

8.3 Validation Commands

Switch# show license

```
License files:
============================================================================
flash:/ma.lic:
  Created Time: Fri Dec  6 17:22:23 CST 2013
  Vendor:       Fiberstore
  Customer:     Fiberstore
  Device MAC:   00:1E:08:09:03:00
  Feature Set:  QINQ MVR ERPS MEF ETHOAM
                VPWS VPLS HVPLS SMLK TPOAM
                OSPF PIM_SM IGMP VRF MPLS
                LDP BGP RSVP OSPF_TE EXTEND_ACL
                PTP BFD SSM IPV6 OSPF6
                PIM_SM6 MVR6 RIPNG TUNNEL_V6
```