
Contents

1 Configuring the FTP Server.....	1
1.1 Introduction.....	1
1.1.1 Overview.....	1
1.1.2 Principles.....	1
1.1.3 Protocols and Standards.....	3
1.2 Configuration Task Summary.....	3
1.3 Configuring Basic Functions of the FTP Server.....	3
1.3.1 Overview.....	3
1.3.2 Procedure.....	3
1.4 Configuring FTP Session Management.....	4
1.4.1 Overview.....	4
1.4.2 Procedure.....	4
1.5 Configuring the FTP Lock Function.....	5
1.5.1 Overview.....	5
1.5.2 Restrictions and Guidelines.....	5
1.5.3 Procedure.....	5
1.6 Enabling AAA on the FTP Server.....	6
1.6.1 Overview.....	6
1.6.2 Restrictions and Guidelines.....	6
1.6.3 Prerequisites.....	6
1.6.4 Procedure.....	6
1.7 Configuring Read/Write Permission Control of FTP Users.....	6

1.7.1 Overview.....	6
1.7.2 Procedure.....	6
1.8 Monitoring.....	7
1.9 Configuration Examples.....	7
1.9.1 Providing the FTP Service in a LAN.....	7

1 Configuring the FTP Server

1.1 Introduction

1.1.1 Overview

File Transfer Protocol (FTP) is a standard application layer protocol formulated by the IETF Network Working Group. It implements file transfer based on Transmission Control Protocol (TCP). FTP is a major method for transferring files on the Internet.

FTP adopts the client/server model. As shown in [Figure 1-1](#), a device can act as an FTP server to provide remote client access and program operations. By issuing commands to the server through the client, you can view the files in the FTP server directory, copy files from a remote computer to the local device, and transfer local files to the server. In addition, FTP provides functions, such as login authentication and read/write access control.

Figure 1-1 FTP Client/Server Mode



1.1.2 Principles

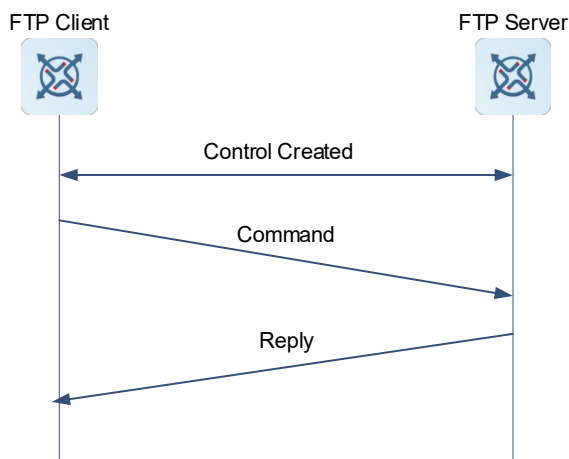
1. FTP Connection

FTP sets up two TCP connections between the client and the server, namely the control connection and the data connection.

- The control connection uses port 21 to transmit control commands, and is always in enabled state.
- The data connection uses port 20 to transmit data. The server can proactively enable or disable the data connection. It sets up a new data connection every time a file or directory is transferred.

For some simple sessions, only the control connection needs to be enabled, the client sends a command to the server, and the server returns a response after receiving the command. The process is shown in [Figure 1-1](#).

Figure 1-1 Control Connection



When the client sends a command for uploading or downloading data, both the control connection and data connection must be established.

2. User Login and Authentication

To access files on the FTP server, the FTP client must have a user account authorized by the FTP server. By default, a device supports configuration of up to 10 users, 2 connections per user, and 10 connections with the server.

In addition, the read and write permissions of files can be defined to effectively prevent unauthorized users from accessing internal files. When the number of a user's FTP login failures reaches the upper limit, the IP address or username used for login is locked. Within a certain period of time, all users cannot log in to the FTP server properly using this IP address or username.

3. Supported FTP Commands

After receiving an FTP connection request, the FTP server requires the client to provide the username and password for authentication.

If the client passes the authentication, the FTP client commands can be executed. The following table lists the FTP client commands supported by the FTP server.

Table 1-1 FTP Client Commands Supported by the FTP Server

ascii	close	mdelete	mput	quit	size
bin	delete	mkdir	nlist	recv	system
bye	dir	mget	passive	rename	type
cd	get	mkdir	put	rmdir	user
cdup	ls	mls	pwd	send	

For how to use these FTP client commands, refer to the documentation of the FTP client software used. In addition, many FTP client tools, such as CuteFTP and FlashFXP, provide the graphic user interface (GUI), which allows users to perform operations without configuring FTP commands.

1.1.3 Protocols and Standards

- RFC959: File Transfer Protocol (FTP)
- RFC3659: Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC2428: FTP Extensions for IPv6 and NATs
- RFC1635: How to Use Anonymous FTP

1.2 Configuration Task Summary

FTP server configuration includes the following tasks:

- (1) Configuring Basic Functions of the FTP Server
- (2) (Optional) [Configuring FTP Session Management](#)
- (3) (Optional) [Configuring the FTP Lock Function](#)
- (4) (Optional) [Enabling AAA on the FTP Server](#)
- (5) (Optional) [Configuring Read/Write Permission Control of FTP Users](#)

1.3 Configuring Basic Functions of the FTP Server

1.3.1 Overview

This section describes how to enable the FTP server and configure the username, password, and top-level directory to provide the FTP service for the FTP client.

1.3.2 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enable the FTP server.

ftp-server enable

The FTP server is disabled by default.

- (4) Configure the top-level directory of the FTP server.

ftp-server topdir *directory*

By default, no top-level directory under which the FTP client can read and write files is configured, that is, the client is prohibited from accessing any directory on the FTP server.

- (5) Configure a username and password for server login.

ftp-server username *username* [**privilege level**] **password** [*type*] *password*

By default, no username and password are configured for login to the FTP server, that is, no login users are restricted.

1.4 Configuring FTP Session Management

1.4.1 Overview

- The FTP login times refers to the number of times that the user's account and password can be verified when the user logs in to the FTP server.
- The FTP login timeout refers to the maximum time that the user can stay online after the username and password are verified. If the username and password are not verified again before login timeout, the session will be terminated to ensure that other users can log in to the FTP server.
- The idle timeout refers to the time from the completion of the last FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command (for example, after a file is completely transferred), the server starts to count the idle time again, and stops counting when the next FTP client command arrives. Therefore, the configuration of the idle timeout does not affect time-consuming file transfer operations.

1.4.2 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Configure FTP session management. Configure at least one of the following tasks.

- Configure the FTP login times.

ftp-server login times *times*

By default, the FTP login times is 3, that is, a session will be terminated once you enter an incorrect username or password so that other users can go online.

- Configure the FTP login timeout.

ftp-server login timeout *time*

By default, the FTP login timeout is 2 minutes.

- Configure the idle timeout.

ftp-server timeout *time*

By default, the idle timeout of an FTP session is 10 minutes.

- Configure the maximum number of FTP sessions.

ftp-server max-sessions *number*

By default, the maximum number of FTP sessions is 20.

1.5 Configuring the FTP Lock Function

1.5.1 Overview

- After the IP address lock function is enabled, if the cumulative number of login failures caused by entry of the incorrect username or password reaches the configured upper limit, the FTP session is terminated and the user's IP address is locked. In addition, all users cannot log in to the FTP server properly using this IP address or username.
- After the username lock function is enabled, if the cumulative number of login failures caused by entry of the incorrect password reaches the configured upper limit, the FTP session is terminated and the username is locked. The user cannot log in to the FTP server, but other users are not affected.
- The FTP lock time refers to the duration that a user needs to wait for automatic unlocking after the user is locked because the number of the user's login failures reaches the upper limit. The locked user can log in to the FTP server only after the login silence time expires.
- The maximum number of login verification times allowed by the FTP lock function refers to the maximum number of times that the username and password of a user can be verified after the FTP lock function is enabled. The default value is 3. If the number of verification failures exceeds the configured upper limit, the session is terminated and the user is locked.

1.5.2 Restrictions and Guidelines

After the IP address lock function is enabled, if the number of locked IP addresses reaches the upper limit, the full lock function is enabled. Then, the FTP server no longer accepts the connection request from any user until the number of locked IP addresses is smaller than the upper limit.

1.5.3 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Configure the FTP lock function. Configure at least one of the following tasks.

- Disable the IP address lock function.

ftp-server login ip-block disable

The IP address lock function is enabled by default.

- Configure the username lock function.

ftp-server login username-block disable

The username lock function is enabled by default.

- Configure the FTP lock time.

ftp-server login silence-time *time*

By default, the FTP lock time is 5 minutes.

- Configure the maximum number of IP addresses that can be locked after the IP address lock function is enabled.

ftp-server login max-block-limit *limit*

By default, up to 30 IP addresses can be locked.

1.6 Enabling AAA on the FTP Server

1.6.1 Overview

By default, FTP does not support AAA login authentication. However, you can enable AAA on the FTP server through configuration.

1.6.2 Restrictions and Guidelines

This command takes effect only after FTP is enabled.

1.6.3 Prerequisites

Enable the AAA function before configuring this command. For details about how to enable AAA, see "Configuring AAA" in *Security Configuration Guide*.

1.6.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enable AAA on the FTP server.

ftp-server authentication { default | name }

By default, FTP does not support AAA login authentication.

1.7 Configuring Read/Write Permission Control of FTP Users

1.7.1 Overview

After the user read/write permission control function is enabled, the configured FTP user levels or AAA username levels can be used to control read/write permissions. By default, users of all levels have the read/write permissions. After permission control is enabled, if the user level is not configured, it is set to 1 by default and the user has only the read permission, that is, the user can only download data. You can configure FTP users of different levels as required for read/write permission control.

1.7.2 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enable read/write permission control of FTP users.

ftp-server login permission enable

By default, read/write permission control of FTP users is disabled.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

Running the **clear** command may lose vital information and thus interrupt services.

Table 1-1 FTP Server Monitoring

Command	Purpose
clear ftp-server block-list [all ip-address { ipv4-address ipv6-address } [vrf vrf_name] username user]	Clears the user lock entries in the FTP lock list.
show ftp-server	Displays the FTP server status information.
show ftp-server { ip-block username-block } list	Displays the user lock entries in the FTP lock list.
debug ftp-server err	Debugs the FTP server error events.
debug ftp-server pro	Debugs the FTP server message events.

1.9 Configuration Examples

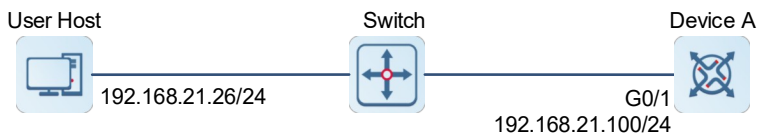
1.9.1 Providing the FTP Service in a LAN

1. Requirements

As shown in [Figure 1-1](#), a device in a LAN acts as the FTP server to provide the upload and download services for users. The switch is an access device. The required session idle timeout is 5 minutes.

2. Topology

Figure 1-1 Providing the FTP Service in a LAN



3. Notes

Configure device A as follows:

- (1) Enable the FTP server function.
- (2) Configure the top-level directory **/syslog**.
- (3) Set the username to **user** and password to **password**.
- (4) Set the session idle timeout to **5** minutes.

4. Procedure

- (1) Configure device A.

- a. Configure an IP address.

```

DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1DeviceA(config-if-
GigabitEthernet 0/1)# ip address 192.168.21.100 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
  
```

- b. Enable the FTP server function.

```
DeviceA(config)# ftp-server enable
```

- c. Configure the top-level directory **/syslog**.

```
DeviceA(config)# ftp-server topdir /syslog
```

- d. Set the username to **user** and password to **password**.

```
DeviceA(config)# ftp-server username user password password
```

- e. Set the session idle timeout to **5** minutes.

```
DeviceA(config)# ftp-server timeout 5
```

- (2) Configure the user host.

Set the IP address of the user host to 192.168.21.26/24.

5. Verification

Run the **show ftp-server** command to view the FTP server configurations.

```

DeviceA# show ftp-server
  ftp-server information
=====
enable : Y
  
```

```
topdir : /syslog
timeout: 5min
total connect: 0
username:user
password:(PLAINTEXT)password
connect num[0]
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface gigabitEthernet 0/1
ip address 192.168.21.100 255.255.255
!
ftp-server enable
ftp-server topdir /syslog
ftp-server timeout 5
ftp-server username user password password
!
```

7. Common Errors

- No username is configured.
- No password is configured.
- No top-level directory is configured.