File Transfer Protocol

File Transfer Protocol

Cisco switches support various protocols for transferring files to and from the device. Among these, FTP and SFTP are commonly used for managing software images, configuration files, and log files.

- File Transfer Protocol (FTP): A standard network protocol used to transfer computer files from one host to another over a TCP-based network. FTP is an unencrypted protocol, meaning data is transferred in plaintext.
- Secure File Transfer Protocol (SFTP): A network protocol that provides file access, file transfer, and file management functionalities over any reliable data stream. It is typically used with the SSH protocol to provide secure, encrypted communication.

FTP

Cisco switches extend FTP client functionalities to support IPv6 networks. This allows the switch to initiate FTP connections using IPv6 addresses, enabling file transfers in IPv6-only or dual-stack network environments. This support is crucial for modern network deployments that increasingly rely on IPv6 for addressing and connectivity.

SFTP

Cisco switches support SFTP client functionality in IPv6 networks. SFTP provides a secure alternative to FTP by encrypting both the data and authentication credentials during transfer. This security is paramount when transferring sensitive information such as configuration files or critical software images over untrusted networks. SFTP leverages the underlying Secure Shell (SSH) protocol for its security features.

Use Cases for File Transfer Capabilities

The FTP and SFTP features on Cisco switches are essential for several key operational tasks.

- Software Image Management: Downloading new Cisco IOS XE software images for upgrades or patching.
- Configuration Management: Backing up current running configurations or restoring previous configurations.
- Log File Retrieval: Transferring system logs and debugging information for analysis.
- File Distribution: Pushing files from the switch to a central server or vice-versa.

Restrictions for File Transfer Operations

This chapter outlines important considerations and limitations when performing file transfer operations (FTP and SFTP) on a Cisco switch.

- Network Connectivity: Ensure full network reachability (routing, firewall rules) between the Cisco switch and the remote FTP/SFTP server.
- Credentials: Valid username and password are required for authentication on the remote FTP/SFTP server.
- Memory Space: Verify that the switch has sufficient flash memory space to accommodate the transferred file, especially for large software images.
- Privilege Levels: Ensure you have the necessary privilege level on the switch to execute file transfer commands.
- File Paths and Names: Specify correct and complete file paths and names on both the source and destination.

FTP Specific Restrictions

- Security: FTP transfers data and credentials in plaintext. Do not use FTP for sensitive information over untrusted networks.
- Port Requirements: Ensure TCP port 21 (control) and dynamic data ports are open if the switch is acting as an FTP client.

SFTP Specific Restrictions

- SSH Dependency: SFTP relies on the SSH protocol. Ensure SSH is enabled and properly configured on the switch and the remote server.
- Authentication: SFTP typically uses username/password or SSH keybased authentication.

IPv6 Specific Restrictions

- IPv6 Enablement: IPv6 routing must be enabled globally on the switch.

- Interface Configuration: Relevant interfaces must have IPv6 addresses configured and be in an up/up state.
- Network Reachability: Ensure IPv6 routing is correctly configured between the switch and the remote IPv6 FTP or SFTP server.

FTP and SFTP transfers

This chapter provides step-by-step instructions for performing client-side file transfer operations using FTP and SFTP on a Cisco switch, including downloading software images.

Before you begin

Verify these prerequisites.

Procedure

Step 1 Verify network connectivity to the remote server. Use **ping** <*remote-server-ip-address*> command to confirm basic IP reachability.

Example:

```
Device# ping 2001:db8::1
```

Replace *remote-server-ip-address* with the actual IP address (IPv4 or IPv6) of your remote FTP or SFTP server.

Step 2 Verify available flash memory space on the switch.

Example:

```
Device# dir flash:
```

Check the "bytes free" to ensure enough space is available for the new file.

Copy file from IPv6 FTP server to flash memory

You can use this task to retrieve configuration files, log files, or software images from a remote IPv6 FTP server.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Enter your password if prompted.

Step 2 Copy the file from the remote IPv6 FTP server to flash memory.

Example:

```
Device# copy ftp://<username>@[<ipv6-
address>]/<path>/<filename> flash:/<destination-filename>

• Replace <username> with the remote FTP server username.
• Replace <ipv6-address> with the IPv6 address of the remote FTP server.
• Replace <path> with the directory path on the remote FTP server.
• Replace <filename> with the name of the file on the remote FTP server.
• Replace <destination-filename> with the desired name for the file on
the switch's flash memory.
• You will be prompted for the password for the remote FTP server.
Note: The IPv6 address must be enclosed in square brackets [] in the URL.

Device# copy ftp://
myuser@[2001:db8:1:1::10]/configs/my_config.txt
flash:/backup_config.txt
Password:
```

Step 3 Verify the file transfer.

Example:

```
Device# dir flash:/<destination-filename>
```

Confirm the file is present in flash memory.

Copy file from SFTP server to flash memory

You can use this task to securely retrieve configuration files, log files, or software images from a remote SFTP server.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Enter your password if prompted.

Step 2 Copy the file from the remote SFTP server to flash memory.

Example:

```
Device# copy sftp://<username>@<server-ip-address>/<
path>/<filename> flash:/<destination-filename>

• Replace <username> with the remote SFTP server username.
• Replace <server-ip-address> with the IPv4 or IPv6 address of the
remote SFTP server.
• Replace <path> with the directory path on the remote SFTP server.
• Replace <filename> with the name of the file on the remote SFTP server.
• Replace <destination-filename> with the desired name for the file on
the switch's flash memory.
```

```
• You will be prompted for the password for the remote SFTP server.
Note: For IPv6 addresses in the URL, enclose them in square brackets [].
```

Example for IPv4 SFTP

```
Device# copy sftp://admin@192.168.1.100/configs/my_config.txt flash:/backup_config.txt
Password:
```

Example for IPv6 SFTP

```
Device# copy sftp://admin@[2001:db8::10]/configs/my_config.txt flash:/backup_config.txt
Password:
```

Step 3 Verify the file transfer.

Example:

```
Device# dir flash:/<destination-filename>
```

Confirm the file is present in flash memory.

Download a software image using FTP (IPv4/IPv6)

You can use this task to upgrade or downgrade the switch's operating system.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Enter your password if prompted.

Step 2 Copy the software image from the remote FTP server to flash memory.

Example:

```
Device# copy ftp://<username>@<server-ip-address>/<
path>/<image-filename.bin> flash:/<imagefilename.
bin>

• Replace <username> with the remote FTP server username.
• Replace <server-ip-address> with the IPv4 or IPv6 address of
the remote FTP server.
• Replace <path> with the directory path on the remote FTP server.
• Replace <image-filename.bin> with the exact name of the Cisco
IOS XE software image file.
• You will be prompted for the password for the remote FTP server.
Note: For IPv6 addresses in the URL, enclose them in square brackets [].
```

Example for IPv4 SFTP

```
Device# copy ftp://ftpuser@
192.168.1.50/software/cisco9k_iosxe.bin
flash:/cisco9k_iosxe.bin
Password:
```

Example for IPv6 SFTP

```
Device# copy ftp://ftpuser@
[2001:db8:a:b::100]/software/
cisco9k_iosxe.bin flash:/cisco9k_iosxe.bin
Password:
```

Step 3 Verify the file transfer.

Example:

```
Device# dir flash:/<image-filename.bin>
```

Confirm the software image file is present.

Download a software image using SFTP

You can use this task to securely upgrade or downgrade the switch's operating system.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Enter your password if prompted.

Step 2 Copy the software image from the remote SFTP server to flash memory.

Example:

```
Device# copy sftp://<username>@<server-ip-address>/<
path>/<image-filename.bin> flash:/<imagefilename.
bin>

• Replace <username> with the remote SFTP server username.
• Replace <server-ip-address> with the IPv4 or IPv6 address of
the remote SFTP server.
• Replace <path> with the directory path on the remote SFTP server.
• Replace <image-filename.bin> with the exact name of the Cisco
IOS XE software image file.
• You will be prompted for the password for the remote SFTP server.
Note: For IPv6 addresses in the URL, enclose them in square brackets [].
```

Example for IPv4 SFTP

```
Device# copy sftp://admin@192.168.1.100/configs/my_config.txt flash:/backup_config.txt
```

Example for IPv6 SFTP

```
Device# copy sftp://admin@[2001:db8::10]/configs/my_config.txt flash:/backup_config.txt
```

Step 3 Verify the file transfer.

Example:

```
Device# dir flash:/<image-filename.bin>
```

Confirm the software image file is present.