FTP and TFTP — Lecture Introduction

- **Lecture** covers FTP, File Transfer Protocol, and TFTP, Trivial File Transfer Protocol
- Both protocols are used to transfer files over a network
- Exam topic 4.9: must be able to describe the capabilities and function of TFTP and FTP in the network
- Must understand the purpose of these protocols and the differences between them, even though their purposes are similar

Lecture Overview

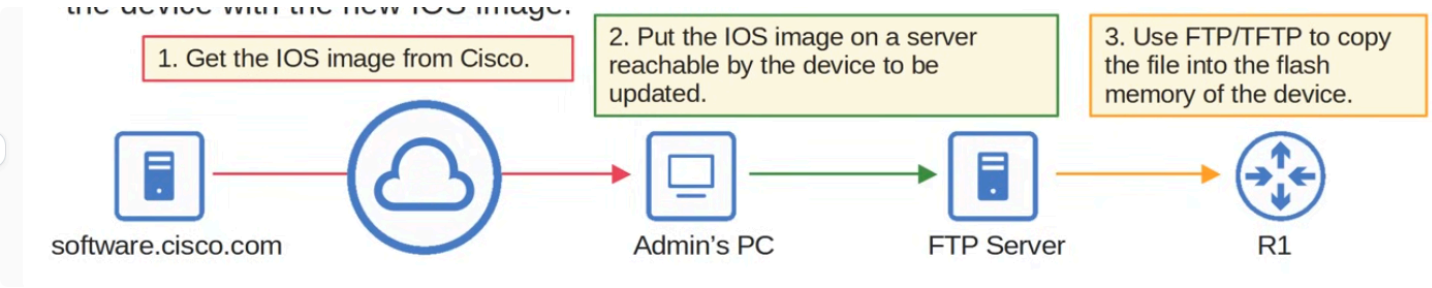
- First: introduce the purpose of FTP and TFTP — the names tell the basic purpose, but a brief overview is given
- Then: compare the two protocols to learn about their functions and how they are different
- Then: introduce the various file systems on Cisco IOS — a basic understanding of how files are stored on Cisco devices is important
- Finally: look at how to use FTP and TFTP in Cisco IOS

Purpose of FTP and TFTP

- FTP, File Transfer Protocol, and TFTP, Trivial File Transfer Protocol, are both industry standard protocols used to transfer files over a network
- Both use a client-server model
- Clients can use FTP or TFTP to copy files from an FTP or TFTP server
- Clients can also use FTP or TFTP to copy files to a server
- As a network engineer, the most common use for FTP and TFTP is in the process of upgrading the operating system of a network device

- You can use FTP or TFTP on the device to download the newer version of IOS and then reboot the device with the new IOS image
- This is not the only use for these protocols — they can be used to transfer all kinds of files between different devices over a network

Example: Upgrading IOS on a Network Device



- Sample network: on the left is a server at software.cisco.com
- The network admin will download the new IOS image from Cisco
- Then he will transfer the IOS image to a server that is reachable by the device he is going to update, which in this example is R1 on the right
- Finally, the network admin will use commands in the CLI of R1 to copy the file into the flash memory of R1
- The last step after that is to reboot R1 using the new version of IOS
- Later in the video, the professor shows how to use the CLI of a Cisco device to transfer files using FTP and TFTP, and then how to reboot the device with the new IOS image to update it

---

TFTP, the Trivial File Transfer Protocol

- TFTP was first standardized in 1981
- It was released after FTP, but is introduced first because TFTP is simpler
- It was named the 'trivial' file transfer protocol because it is simple and has only basic features when compared to FTP
- It only allows a client to copy a file to or from a server — nothing else, just simple file transfers
- It was released after FTP, but it is not a replacement for FTP

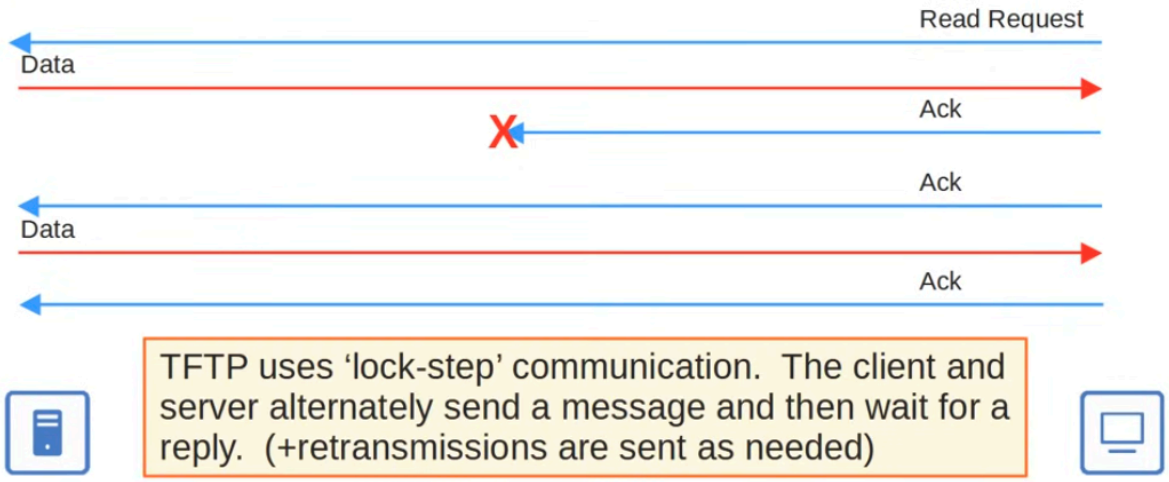
- It is just another tool to use when a lightweight, simple protocol is more important than advanced functionality
- TFTP doesn't use any authentication, meaning no usernames and passwords
- Servers will respond to all TFTP requests because there is no username or password to check
- There is no encryption, so all data is sent in plain text
- Because of this lack of security, TFTP is best used in a controlled environment to transfer small files quickly
- Example: You probably shouldn't use TFTP to transfer important files over the Internet
- TFTP servers listen on **UDP port 69**
- When clients initiate communications with the server, they will use UDP port 69 as the destination port
- UDP is connectionless and doesn't provide reliability using retransmissions
- However, TFTP actually has similar built-in connection and reliability features within the TFTP protocol itself

---

TFTP — Reliability

- TFTP provides reliability using acknowledgments and retransmissions
- Every TFTP data message is acknowledged
- If the client is transferring a file to the server, the server will send Ack messages, one for each data message
- If the server is transferring a file to the client, then the client will send Ack messages, one for each data message from the server
- Timers are used, and if an expected message isn't received in time, the waiting device will re-send its previous message

Example: TFTP Acknowledgement and Retransmission



- The PC on the right is a TFTP client, and the server on the left is a TFTP server
- To download a file from the server, the client sends a 'read request' message
- The server then replies with a data message, containing part of the file
- The client replies with an Ack, but for some reason the message doesn't reach the server
- Because the client sent the Ack, it is waiting for the next data message, but it doesn't come
- So, the client retransmits the Ack message, which successfully reaches the server
- The server then replies with the next data message, and the client replies with an Ack
- This exchange will continue until the client has received the entire file
- This is called 'lock-step' communication
- The client and server alternately send a message and then wait for a reply, send a message, wait for a reply, etc.
- The server will never send two data messages in a row, for example, except in the case of retransmission
- This method of reliability isn't as efficient as TCP's forward acknowledgment and sliding window, but it gets the job done

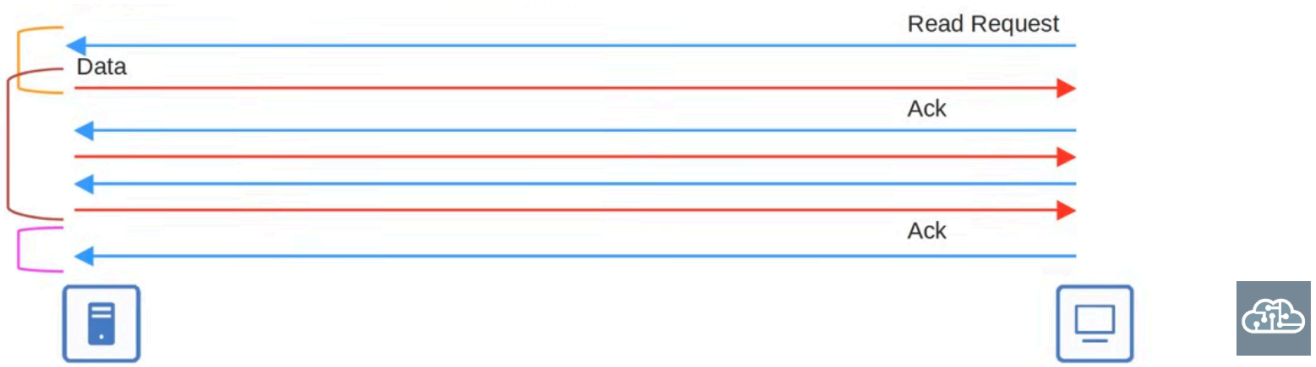
---

TFTP — Connections

- TFTP file transfers have three phases

- First, the connection phase: the client sends a request to the server, and the server responds back, initializing the connection
- Then the data transfer occurs, and data and acknowledgment messages are exchanged
- After the last data message, a final Ack message is sent, terminating the connection

Example: TFTP Connection Phases



- The client sends a request, and the server replies by sending the first data packet
- The connection is officially established
- The client responds with an Ack, and there is an exchange of data packets and Acks
- These messages, including the first data packet, are the data transfer portion of the file transfer
- Finally, the client sends an Ack for the last data packet, and the connection is terminated
- Although TFTP doesn't use TCP, it does have a basic way of managing connections within the protocol itself

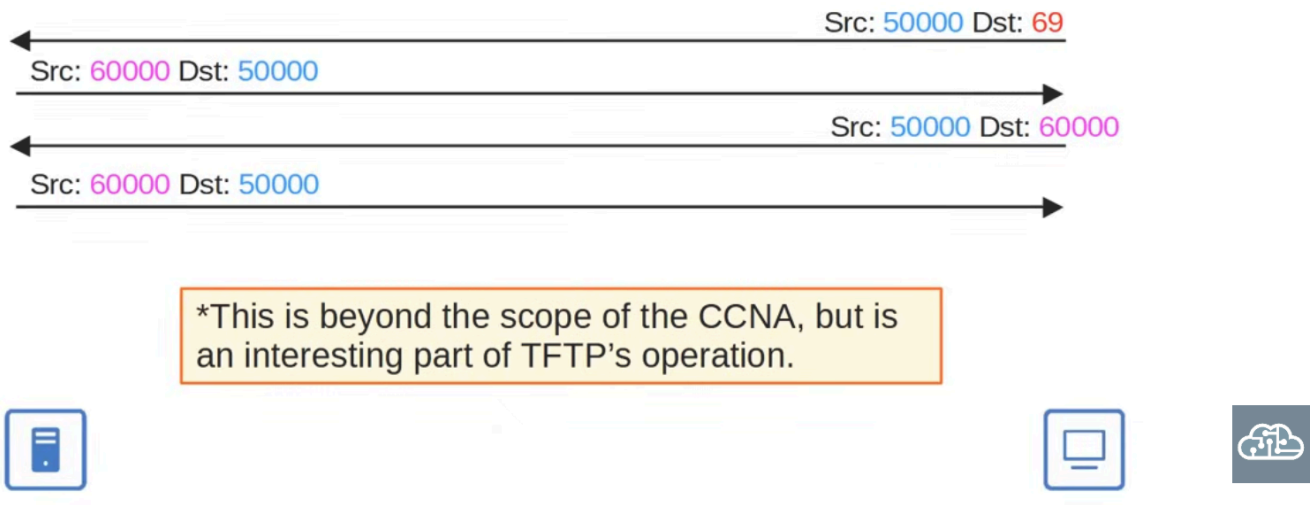
---

TFTP — Transfer Identifiers (TIDs)

- This is an interesting part of TFTP's operation, but it isn't something you have to know for the CCNA exam
- When the client sends the first message to the server, the destination port is UDP port 69 and the source is a random ephemeral port
- In TFTP, this random port is called a 'Transfer Identifier', TID, and is used to identify that particular data transfer

- The server then also selects a random TID to use as the source port when it replies — it doesn't use port 69 as the source port
- When the client sends the next message, the destination port will be the server's TID, again not 69

Example: TFTP Port Usage



- The client sends a message to the server with a random source port and a destination port of 69
- When the server replies, instead of using 69 as the source port, it also uses a random port
- Then the client replies, and uses that random port as the destination port — it no longer uses port 69
- The devices continue to use these two random ports throughout the data transfer
- TFTP's well-known port of 69 is only used in the very first message from the client to the server
- This is beyond the scope of the CCNA, but it's an interesting part of TFTP's operation

---

FTP, the File Transfer Protocol

- FTP was first standardized in 1971

- This is actually before TCP and IP, so FTP is a very old protocol, although it has of course been updated since
- FTP uses TCP ports 20 and 21, instead of just a single well-known port
- Unlike TFTP, usernames and passwords are used for authentication
- However, just like in TFTP, there is no encryption — everything is sent in plain text, including the username and password
- For greater security, FTPS, FTP over SSL/TLS, can be used
- This protocol is also called FTP Secure
- Another option is SSH File Transfer Protocol, SFTP
- Note: FTPS is an upgrade to FTP, adding greater security, whereas SFTP is a different protocol that just has a similar name
- FTP is more complex than TFTP and allows not only file transfers, but clients can also navigate file directories, add and remove directories, list files, etc.

Example: TFTP's Limited Functionality Compared to FTP

- In TFTP, the client could only tell the server 'give me this file' or 'take this file'
- It couldn't even ask the server 'what files do you have?'
- The client sends FTP commands to the server to perform FTP's functions
- There are many different FTP commands, and you can view a list of them on Wikipedia if you're interested

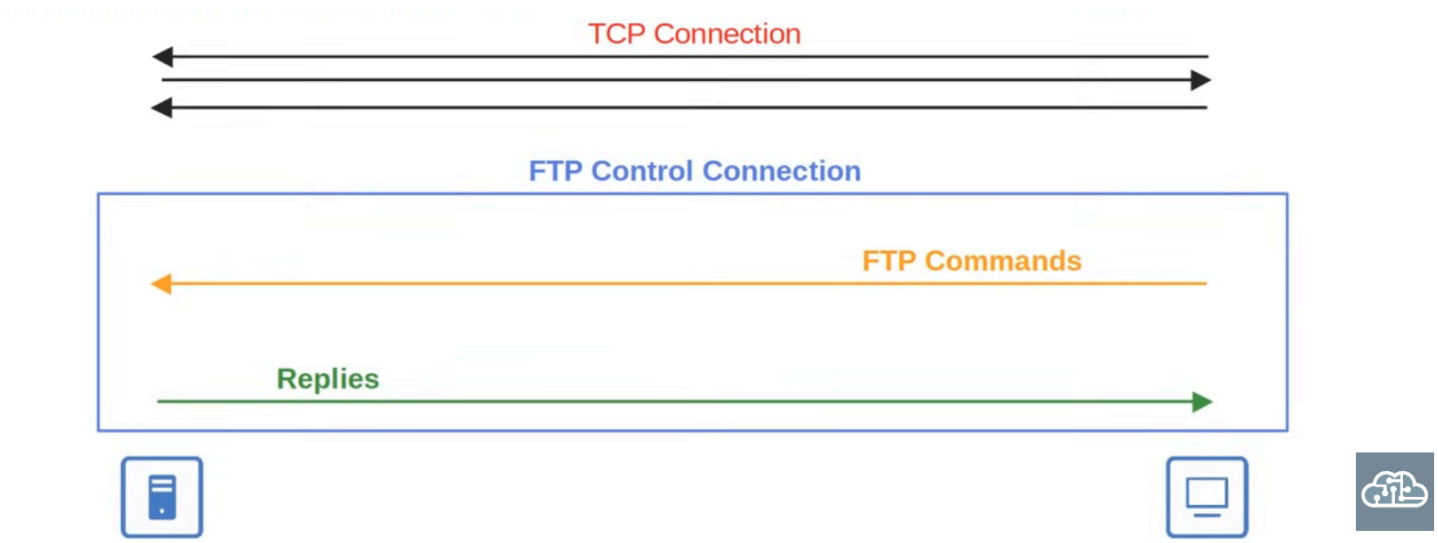
---

FTP — Ports and Connections

- FTP uses two different well-known ports: TCP ports 20 and 21
- That's because FTP uses two types of connections
- An FTP control connection to TCP port 21 is established and used to send FTP commands
- The client sends commands when it wants to perform an action, such as retrieving a file from the server, and the server sends replies to acknowledge
- However, the actual data transfer isn't done using this control connection

- When files or data are to be transferred, separate FTP data connections to TCP port 20 are established and terminated as needed

Example: Establishing the FTP Control Connection



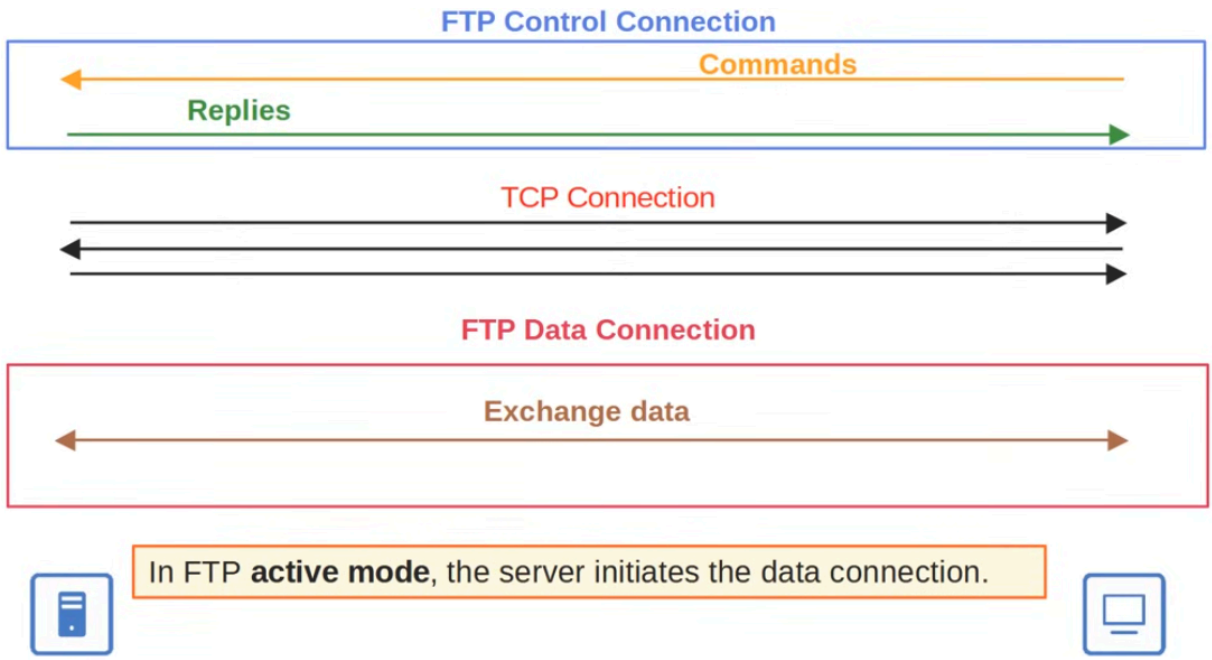
- The client initiates the TCP connection, and the usual SYN, then SYN-ACK, then ACK exchange is used
- Now the FTP control connection is established
- The client will send FTP commands to the server, for example to say that the PC wants to get a file from the server
- The server replies to acknowledge the command
- But now we need an FTP data connection to actually transfer the data

---

FTP — Data Connection Modes

- There are two different modes which can be used to establish an FTP data connection

FTP Active Mode



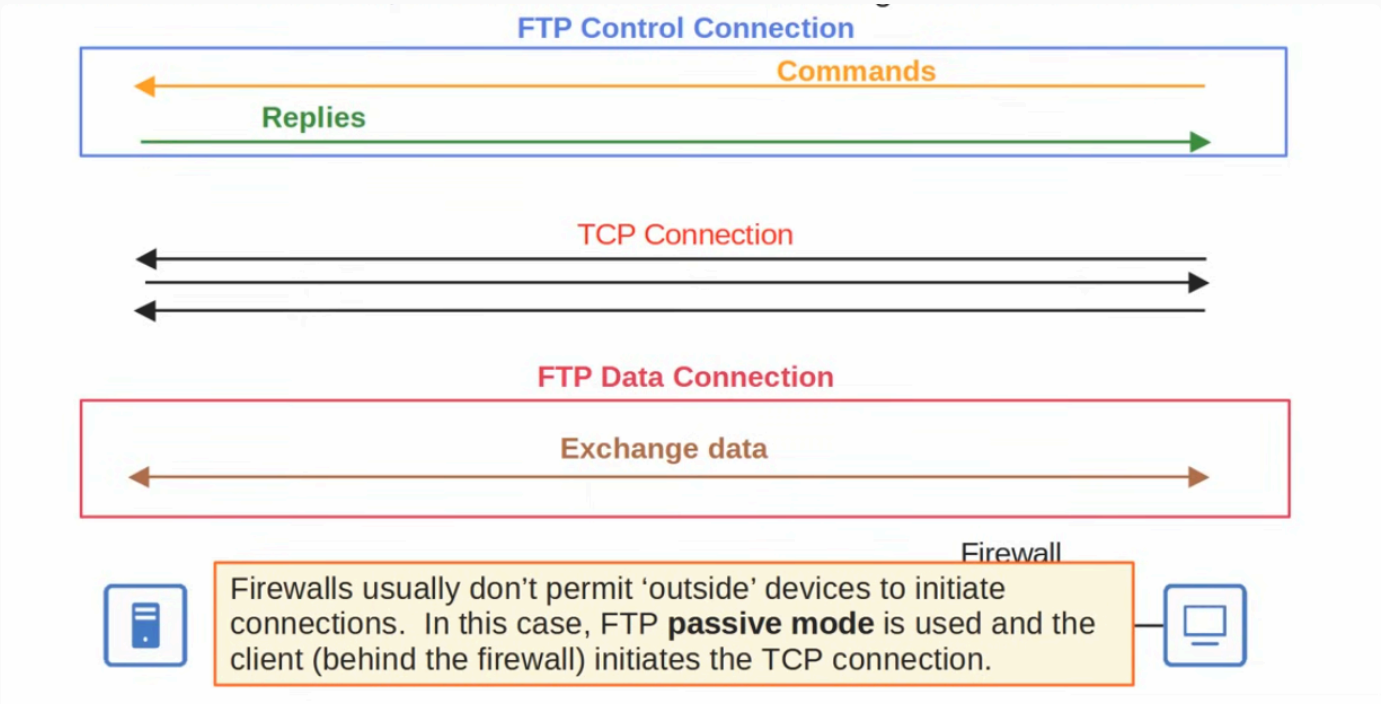
- The default method of establishing FTP data connections is active mode, in which the server initiates the TCP connection
- Example: FTP Active Mode
  - The first arrow, which would be the initial TCP SYN message, is from the server to the client
  - Now the FTP data connection is established, and the data can be exchanged
- The point to remember: in FTP active mode, the server initiates the data connection
- Note: the FTP control connection is maintained throughout this whole process
- It isn't terminated, so there are two active connections

FTP — Data Connection Modes (Continued)

FTP Passive Mode

- Active mode is considered the 'normal' mode of initiating FTP data connections
- However, the network has changed: the client is now behind a firewall
- In FTP passive mode, the client initiates the data connection
- This is often necessary when the client is behind a firewall, which could block the incoming connection from the server

- Example: FTP Passive Mode with a Firewall



  - The first message in the TCP connection is initiated by the client
  - The firewall permits the server's replies
  - The firewall would block the message if the server tried to initiate the TCP connection itself
  - Once the FTP data connection is established, the data is exchanged
- Key point to remember: firewalls usually don't permit 'outside' devices to initiate connections
- In this case, FTP passive mode is used and the client, which is behind the firewall, initiates the TCP connection
- Note: if you're interested in learning more about firewalls, consider studying for the CCNP security certification at some point in the future

FTP and TFTP — Comparison

FTP	TFTP
-Uses TCP (20 for data, 21 for control) for connection-based communication	-Uses UDP (69) for connectionless communication (although a basic form of 'connection' is used within the protocol itself)
-Clients can use FTP commands to perform various actions, not just copy files	-Clients can only copy files to or from the server
-Username/PW authentication	-No authentication
-More complex	-Simpler

- FTP is more complex than TFTP, and it would take a long time to really cover all there is to know about FTP
- FTP uses TCP for connection-based communication
- Port 20 is used for data connections, and port 21 is used for control connections
- TFTP uses UDP port 69 for connectionless communication, although there is a basic form of connection within the protocol itself
- FTP clients can use commands to perform various actions, not just copy files
- TFTP clients can only copy files to or from the server — they can't delete files, list files, etc.
- FTP uses usernames and passwords to limit who can access the server
- TFTP has no authentication system at all
- So, FTP is a more complex protocol, and TFTP is simpler

IOS File Systems

- This is a very brief introduction, just this slide, because we will be looking at transferring files from TFTP and FTP servers onto a Cisco IOS device

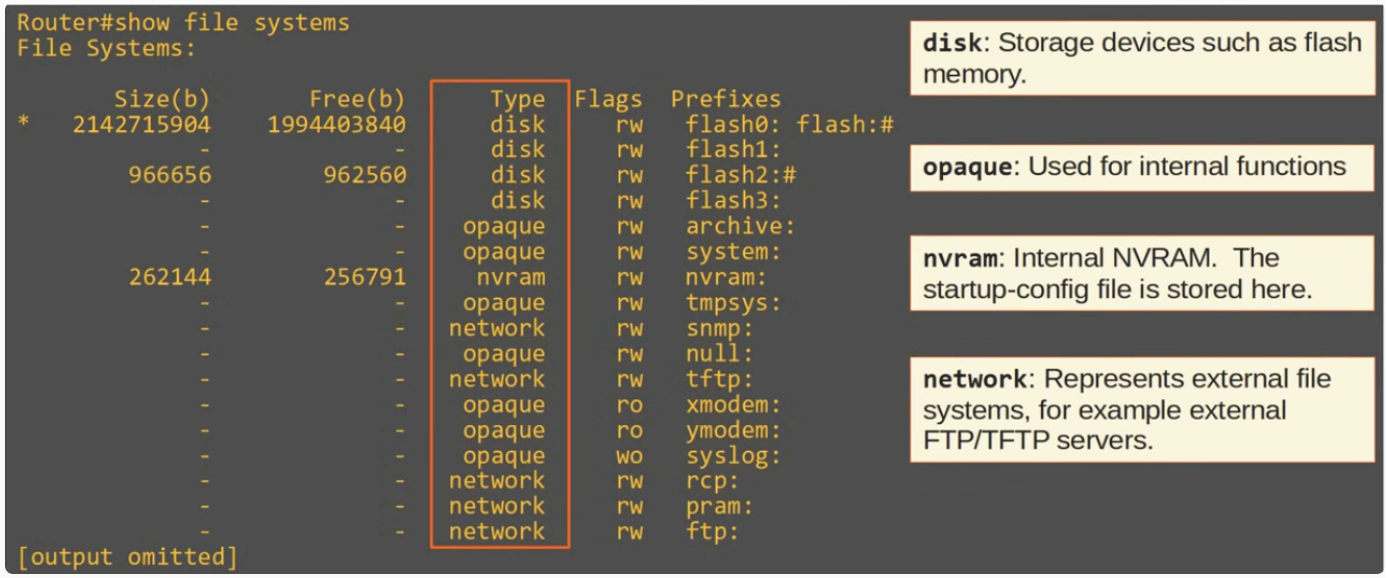
- A file system is a way of controlling how data is stored and retrieved
- If you have a PC, it certainly has its own file system
- You can view the file systems of a Cisco IOS device with the command **`show file systems`**

Verification:

```
show file systems
```

- There are quite a few file systems, and the professor even cut out a few because the output was too long

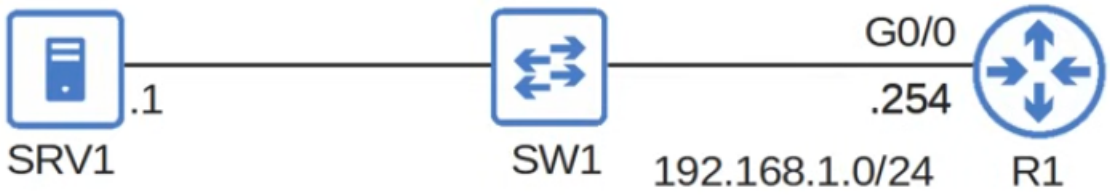
- There are different types of file systems:



  - The disk type refers to storage devices such as flash memory
    - This is usually where the Cisco IOS file itself is stored
    - When the device boots up, it copies the IOS file from flash into RAM
  - The opaque disk type is used for specific internal functions
    - These refer to logical internal systems, not actual separate storage devices
  - The NVRAM type refers to the NVRAM, non-volatile RAM, of the device
    - Normal RAM loses all of its data when the device loses power
    - However, NVRAM does not
    - The startup-config file is stored in NVRAM
  - There is also the network type
    - This represents external file systems, for example FTP or TFTP servers
- Note: the professor doesn't think you'll find any questions about these file systems on the exam — the topic was removed in the newest version of the CCNA
- This introduction ends here
- Next: how to use TFTP and FTP to transfer files into the flash memory of Cisco devices

Using TFTP and FTP in Cisco IOS

Demonstration Network Overview



- Simple network used to demonstrate TFTP and FTP
- R1 is a Cisco router running Cisco IOS
- A new version of IOS has been downloaded and saved on SRV1
- SRV1 is a server running both TFTP and FTP
- The goal is to try out both TFTP and FTP to get the new version of IOS from SRV1 onto R1

```
R1#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
[output omitted]
```

- You can view the contents of flash with **`show flash`**

```
R1#show flash
System flash directory:
File  Length   Name/status
  3   33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

- First, you can view the current version of IOS running on R1 with `show version`
- In the output, you can see the image name, C2900-UNIVERSALK9-M
- Notice the K9, meaning it supports cryptographic features like SSH
- Then the version number, 15.1(4)M4
- Note: perhaps in a future video the professor will talk about the naming conventions of IOS versions, but it is skipped over for now

- The output of `show version` is actually quite long — the professor is just showing the top portion
- Note: for simplicity's sake, the professor is using Packet Tracer for this demonstration, although usually GNS3 is used
- You can also view the contents of flash with `show flash`

Verification:

```
show version
```

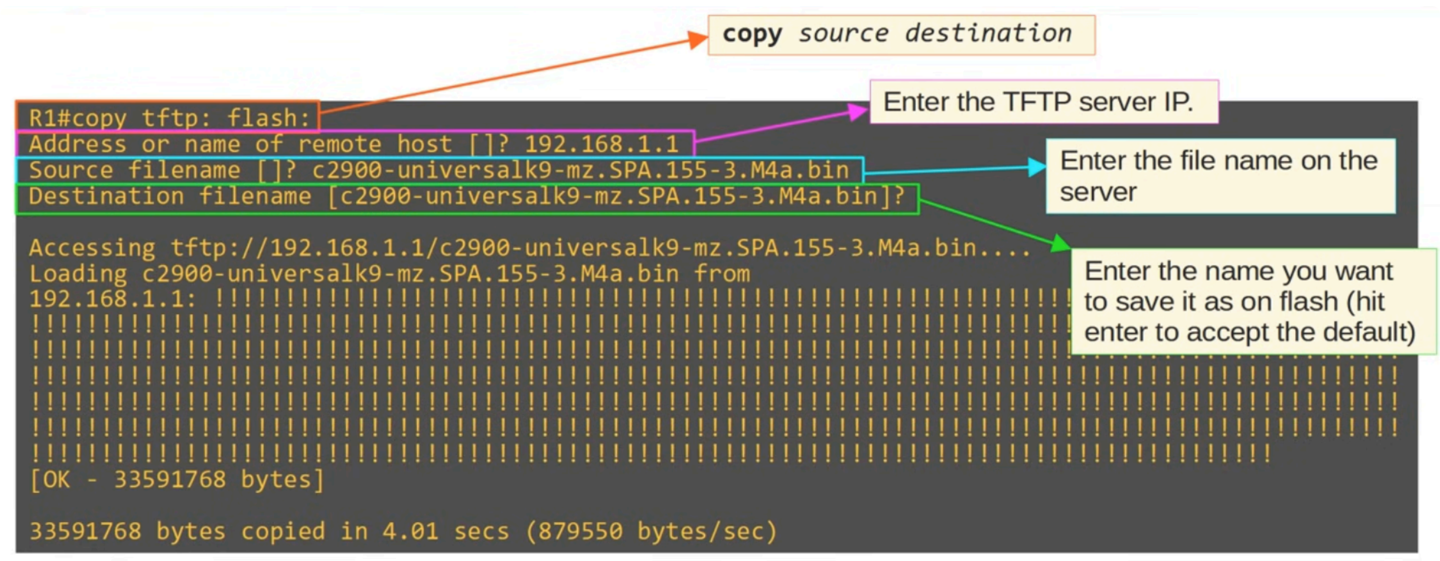
Verification:

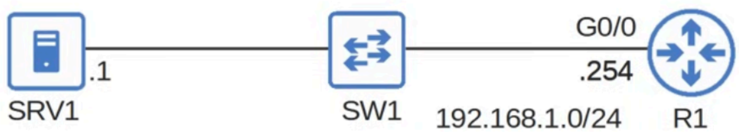
```
show flash
```

- The plan: use TFTP to copy a new version of IOS from SRV1 to the flash of R1, configure R1 to boot with the new version of IOS, and then finally delete the old version from flash

---

Copying a File using TFTP





- The command is `copy`, followed by the source and the destination
- By using TFTP as the source, you tell the router that you want to access a TFTP server
- The router then asks you for the IP address of the remote host
  - This is where you enter the TFTP server's IP address
- Then enter the source filename, the name of the file you want to download
  - Note: you have to know this beforehand — TFTP isn't capable of asking a server 'what files do you have?'
  - The professor already knew the name of the file on the server, so he entered it
- Then you're asked what name you want to save the file as on the router
  - You can just hit enter to accept the default name, which is the same name as on the TFTP server

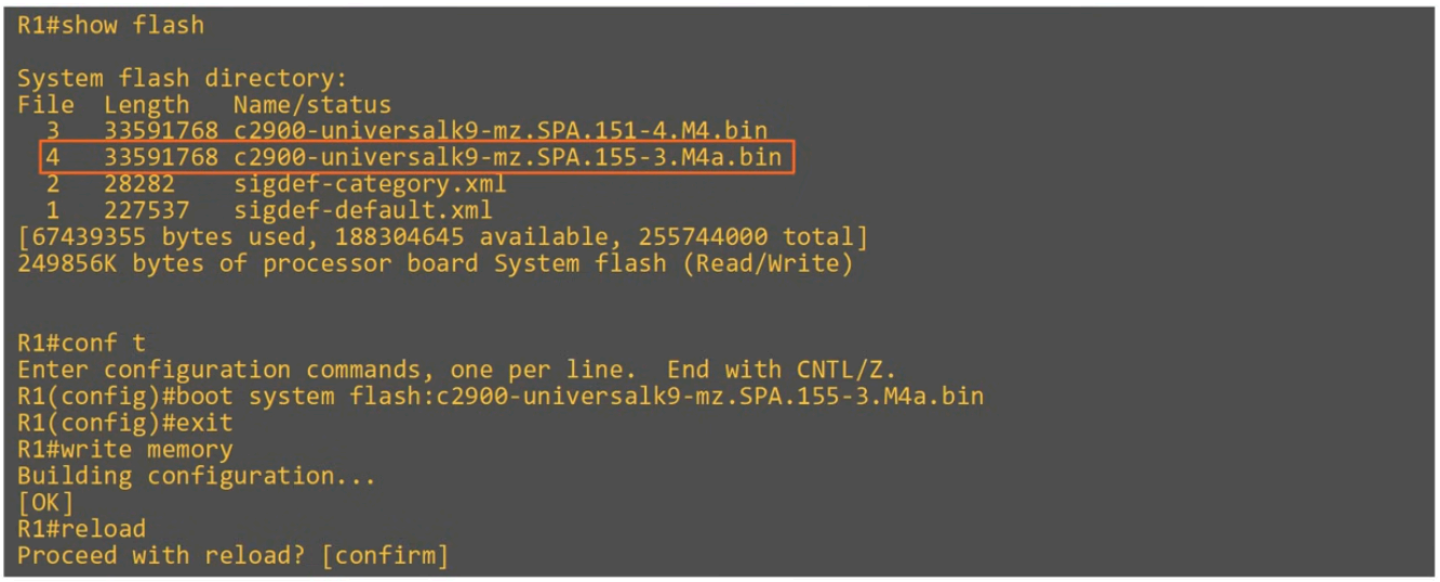
Command:

```
copy tftp: flash:
```

- And that's it, the file is then transferred from the TFTP server to the router

---

Configuring R1 to Boot with the New IOS



- The professor used `show flash` to check the contents of flash
- Here you can see the new version of IOS that was copied from the TFTP server

Verification:

```
show flash
```

- Now, to make the router use this file as its OS instead of the old file:
- From global config mode, use the command `boot system`, followed by the filepath

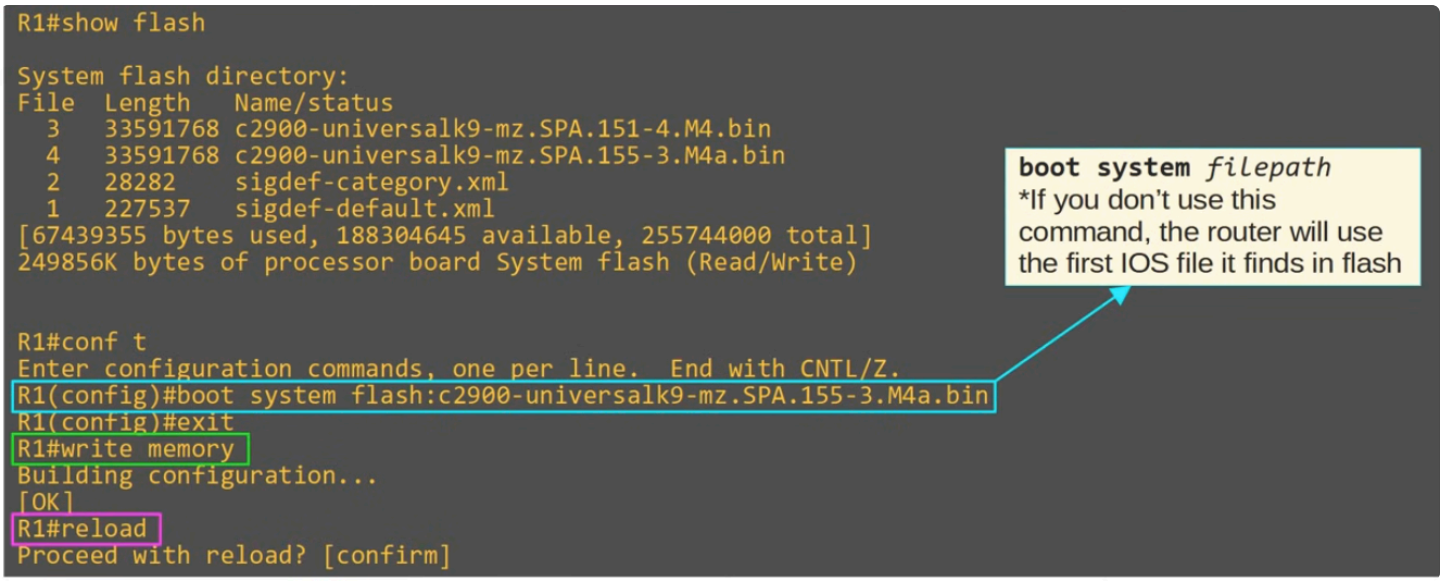
Command:

```
R1#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
  4   33591768 c2900-universalk9-mz.SPA.155-3.M4a.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[67439355 bytes used, 188304645 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#boot system flash:c2900-universalk9-mz.SPA.155-3.M4a.bin
R1(config)#exit
R1#write memory
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
```

boot system *filepath*
*If you don't use this command, the router will use the first IOS file it finds in flash

```
R1(config)# boot system
```

- Note: if you don't use this command, the router will boot using the first IOS file it finds in flash
- So, you should use this command to force it to use the newer version
- After that, make sure you save the configuration before reloading the device, or the `boot system` command won't take effect



- Then simply use the `reload` command to restart the device

Command:

```
R1# reload
```

```
R1#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.5(3)M4a, RELEASE SOFTWARE(fc1)
[output omitted]

R1#delete flash:c2900-universalk9-mz.SPA.151-4.M4.bin
Delete filename [c2900-universalk9-mz.SPA.151-4.M4.bin]?
Delete flash:/c2900-universalk9-mz.SPA.151-4.M4.bin? [confirm]

R1#show flash

System flash directory:
File  Length   Name/status
  4   33591768 c2900-universalk9-mz.SPA.155-3.M4a.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

- After the device finished restarting, the professor used `show version` to check the running version of IOS
- R1 is now using the new version, 15.5, instead of the old one, 15.1

Verification:

```
show version
```

Deleting the Old IOS Image

```
R1#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.5(3)M4a, RELEASE SOFTWARE(fc1)
[output omitted]

R1#delete flash:c2900-universalk9-mz.SPA.151-4.M4.bin
Delete filename [c2900-universalk9-mz.SPA.151-4.M4.bin]?
Delete flash:/c2900-universalk9-mz.SPA.151-4.M4.bin? [confirm]

R1#show flash

System flash directory:
File  Length   Name/status
  4   33591768 c2900-universalk9-mz.SPA.155-3.M4a.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

- Finally, let's delete the old version of IOS — it's not needed anymore, it's just taking up space on the device
- The command to delete a file is **`delete`**, followed by the filepath
- It asks you to confirm, so the professor did

Command:

```
R1# delete
```


```
R1#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.5(3)M4a, RELEASE SOFTWARE(fc1)
[output omitted]

R1#delete flash:c2900-universalk9-mz.SPA.151-4.M4.bin
Delete filename [c2900-universalk9-mz.SPA.151-4.M4.bin]?
Delete flash:/c2900-universalk9-mz.SPA.151-4.M4.bin? [confirm]

R1#show flash

System flash directory:
File  Length   Name/status
  4   33591768 c2900-universalk9-mz.SPA.155-3.M4a.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

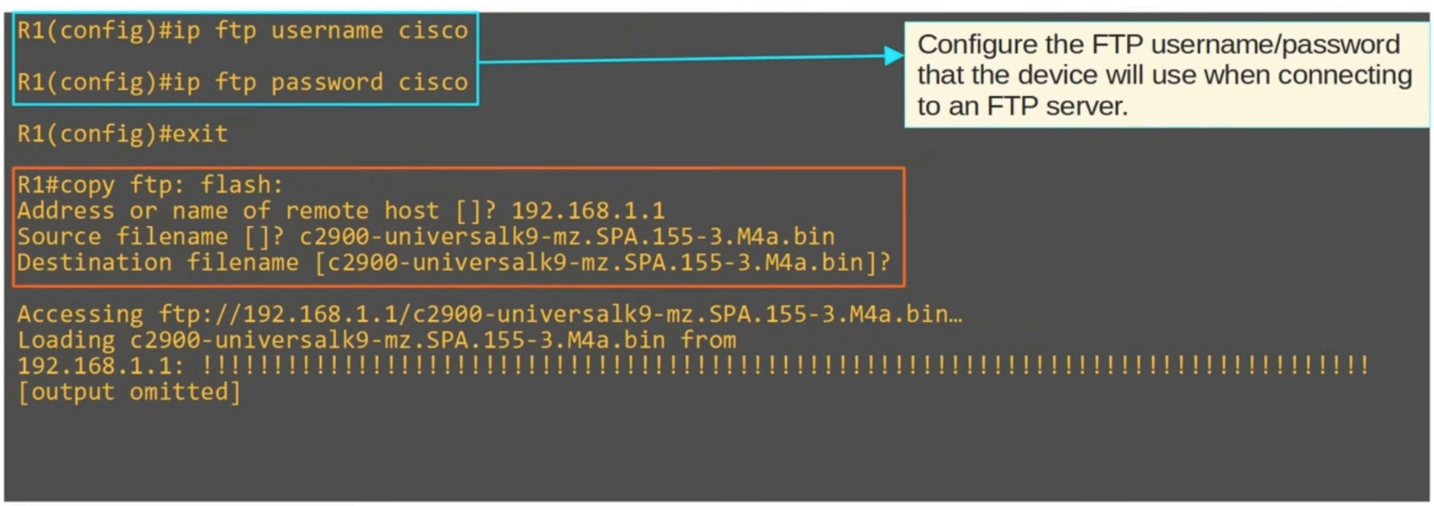
- Then the professor used `show flash` to view the contents of flash, and now the old file is gone

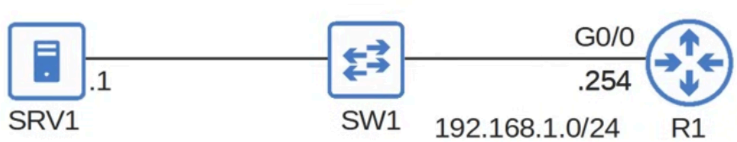
Verification:

```
show flash
```

- Summary of what was accomplished:
    - Successfully used TFTP to copy an IOS file to R1 from a TFTP server
    - Configured R1 to boot using that IOS file
    - Reloaded R1
    - Deleted the old IOS image from the device

Using FTP in Cisco IOS





- The professor will only show the process of transferring the file from the server to the router, because the rest is the same
- Once the file is on the device, the other steps such as the `boot system` command, deleting the old file, etc., are all the same
- First, you should configure the username and password that the router will use when connecting to an FTP server
- Remember, FTP authenticates using a username and password
- So, this same username and password must be configured on the server, too
- In this case, the professor configured the username and password as **cisco**
- Then the copy command itself is basically the same
- `copy ftp: flash:` — then enter the FTP server's IP address, the source filename, and the name you want to save the file as on the local router

Command:

```
copy ftp: flash:
```

- That's it
- Then to upgrade the IOS, you could use the same `boot system` command, save the config, and reload the router

---

Cisco IOS File & Boot Commands — Quick Reference

Command	What it does
`show file systems`	Shows available storage locations/file systems such as **Flash, NVRAM, and USB**.
`show version`	Shows the **IOS version**, device uptime, hardware info, and boot information.
`show flash`	Shows the **files stored in Flash memory**, including IOS images.
`copy <source> <destination>`	Copies a file from one location to another.
`boot system <filepath>`	Tells the router **which IOS image to load when it boots**.
`ip ftp username <username>`	Sets the username the router uses when connecting to an **FTP server**.
`ip ftp password <password>`	Sets the password used to connect to an **FTP server**.

- Here are the commands we just used — if you don't remember any of these commands, go back in the video to review
- The professor also wants to say something about the COPY command
- This actually isn't the first time we've seen that command
- Previously, the professor introduced it as `copy running-config startup-config`, as a method to save the configuration of the device

Command:

```
R1# copy running-config startup-config
```

- It copies the source, the current running config, to the destination, the startup config

---

Review Before the Quiz

- First, the purpose of FTP and TFTP — basically, they allow you to transfer files between devices over a network
- Then the professor gave an overview of TFTP and FTP, and compared the two
  - TFTP is simpler and useful for quickly transferring small files in a controlled environment, but has no advanced functionalities or any security features
  - FTP has much greater functionality, and includes username and password authentication
  - If you use FTPS, it has many other security benefits, but that's out of the scope of this video
- Then the professor very briefly introduced the file systems in Cisco IOS
- Finally, the professor showed how to use TFTP and FTP to get a new IOS file from a server, and then reboot the device with the new version of IOS
