**Day-1**

Servers and PCs are connected to the switch.

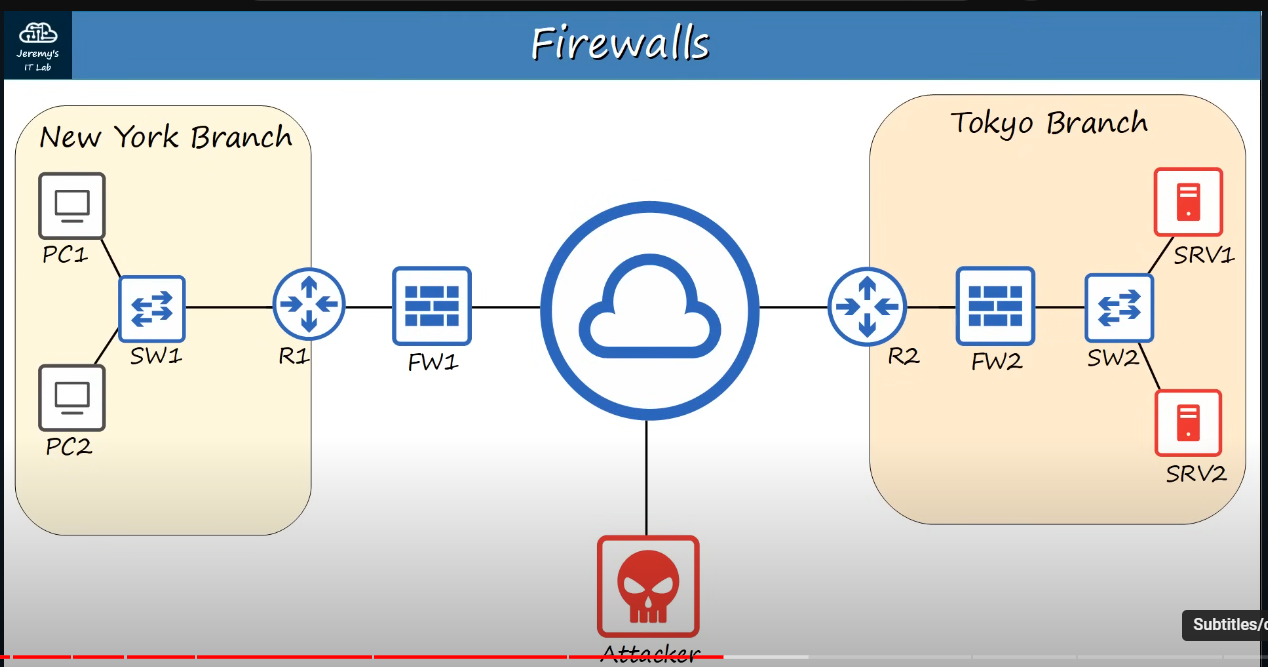
CISCO catalyst switch : Catalyst 9200 , Catalyst 3650

Router is used to connect the switches between two different LANs or two branches (Tokyo and Newyork)

CISCO router : ISR 1000, ISR 900, ISR 4000

Routers have few network interfaces than switches.

Note: Switches are used to forward data within a LAN. Routers do the opposite. Routers are used to provide connectivity between LANs. Routers are therefore used to send data over the Internet.



**Networking Firewalls:**

Firewalls are specialty network security devices that control network traffic entering and exiting your network. Firewall can be places outside of your router like FW1, or inside of network like FW2.

CISCO Firewalls : ASA5500-X, Firepower 2100(next generation firewall).

Firewalls monitor and control network traffic based on configured rules.

Firewall are known as “Next-Generation Firewalls” when they include more modern and advanced filtering capabilities.

**Host-Based Firewalls:**

Host-based firewalls are software applications that filter traffic entering and exiting a host machine, like a PC.

**Day-2**

Switches have ports and these ports are also known as Interfaces.

Bits and Bytes

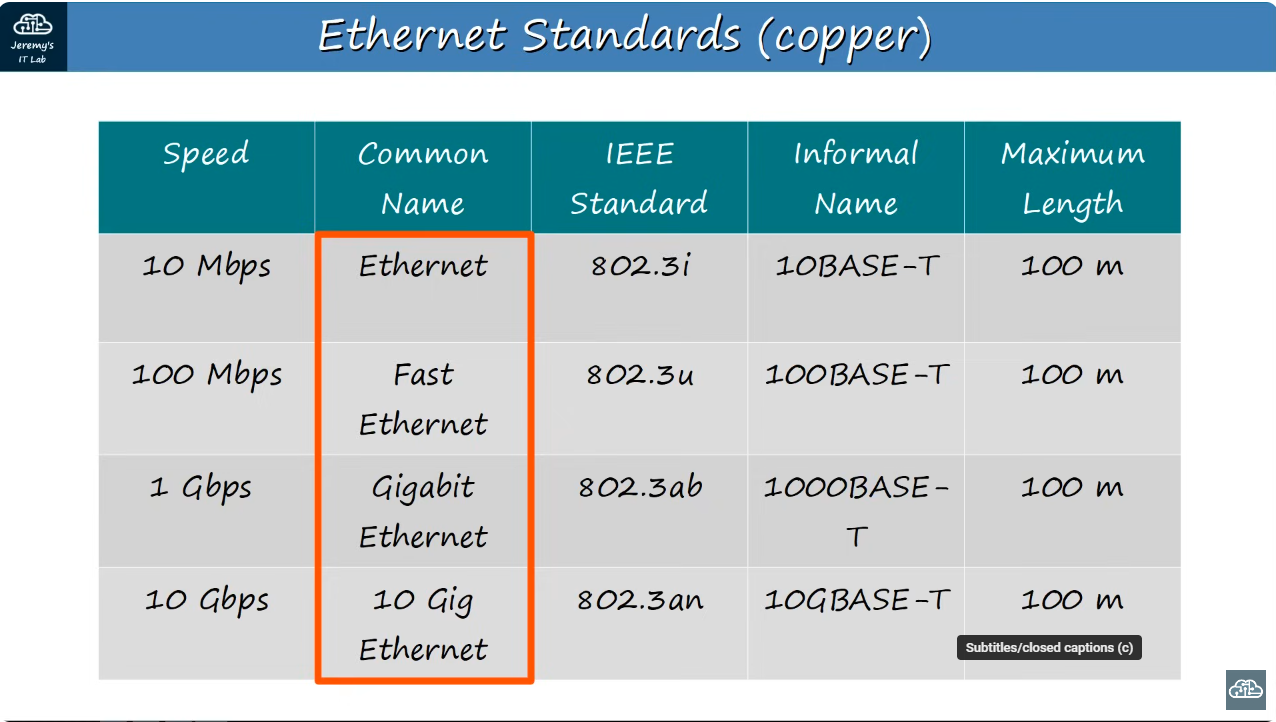
* 1 kilobit (Kb) = 1,000 bits
* 1 megabits (Mb) = 1,000,000 bits
* 1 gigabit (Gb) = 1,000,000,000 bits
* 1 terabit (Tb) = 1,000,000,000,000 bits

Note

* 1 byte = 8 bits

Ethernet Standards (copper)

IEEE 802.3 standards in 1983. Example: 10BASE-T and here T means Twisted Pair Cable.



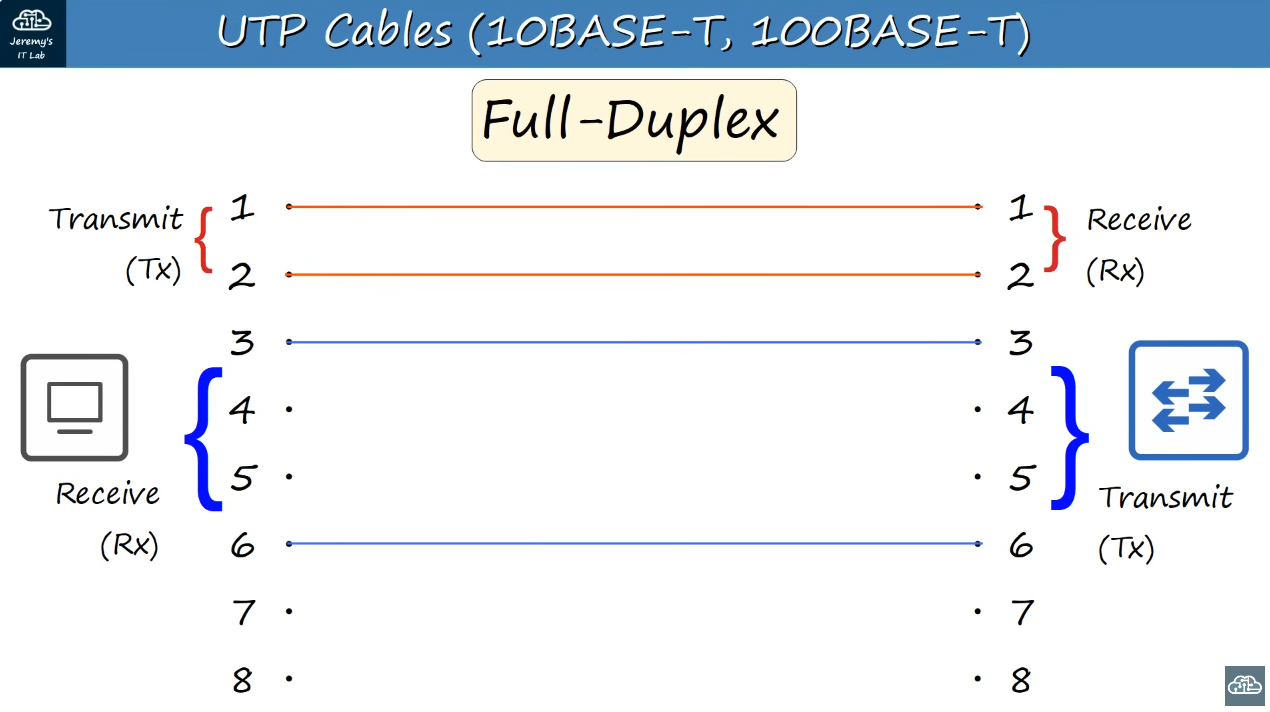
UTP (Unshielded Twisted Pair)

Example RJ-45

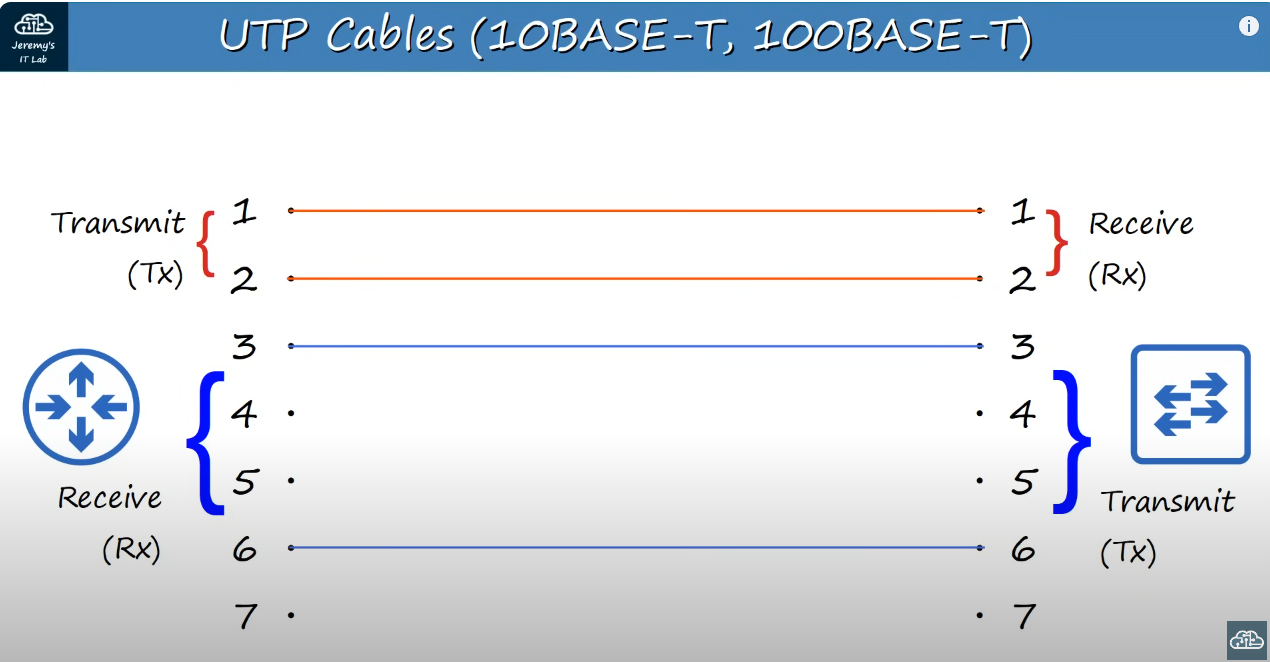
Other

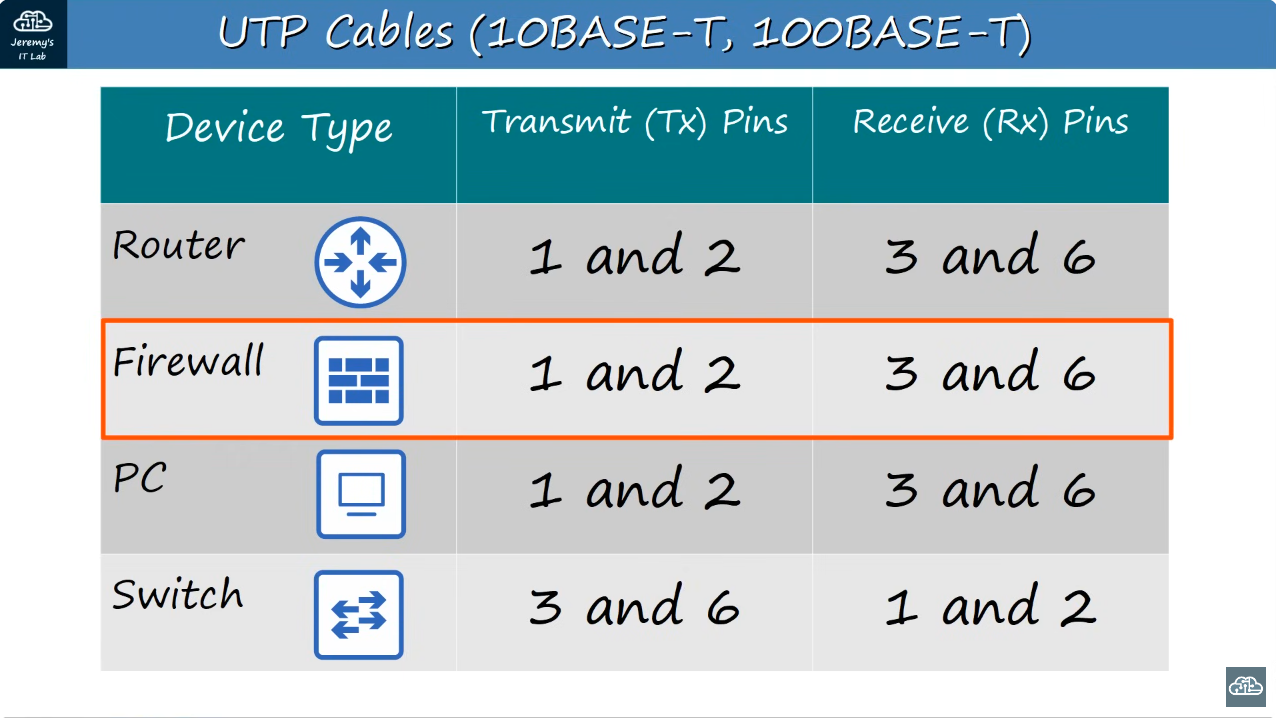
10BASE-T

100BASE-T both have 2 pairs or we can say 4 wires.



Duplex means both device can send data at the same time.

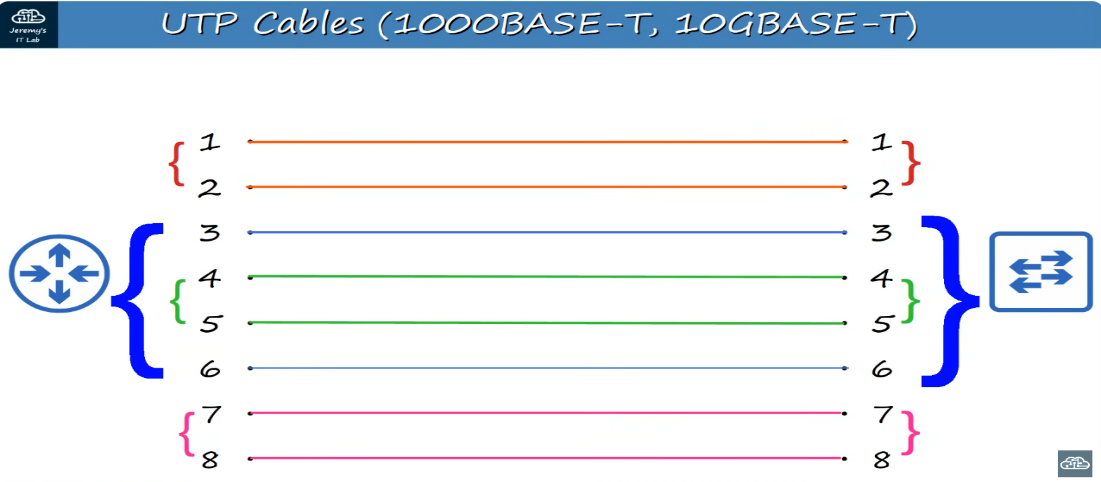




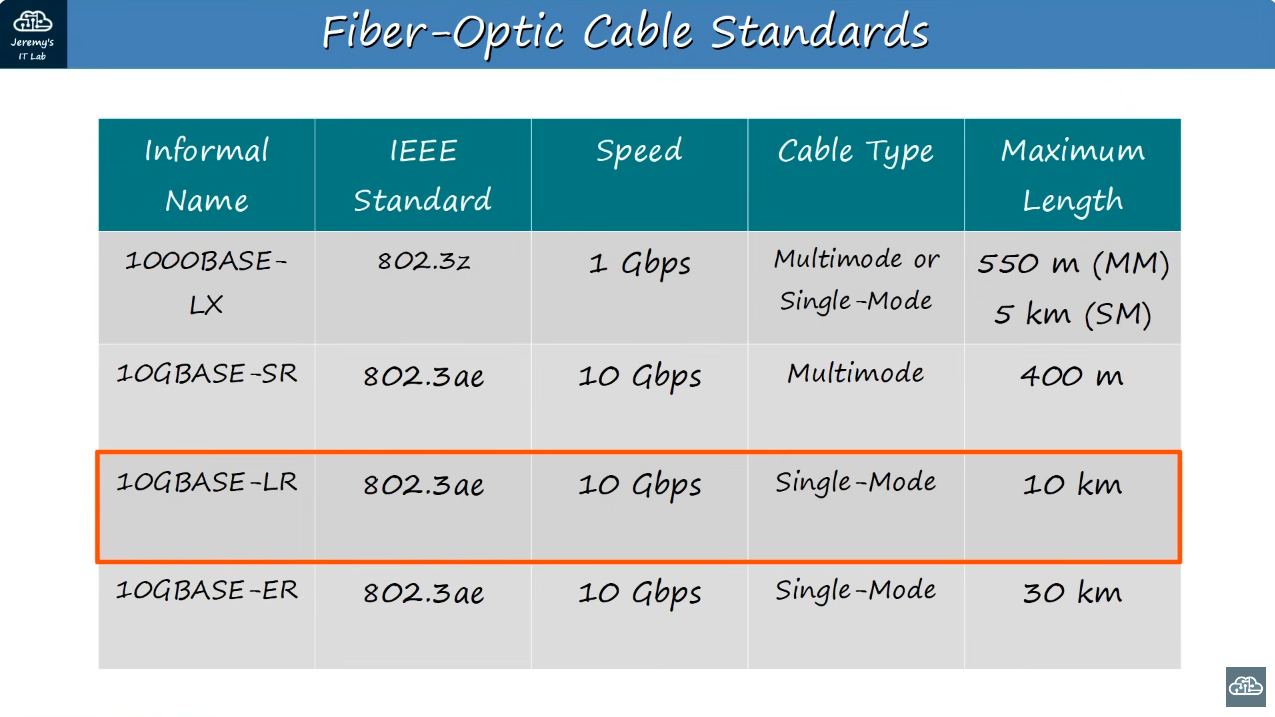
We can see that the if two different end have router and switch then router sends the data from 1 and 2 pin which is received by the switch from pin 1 and 2. Therefore, they needed the straightforward cable.

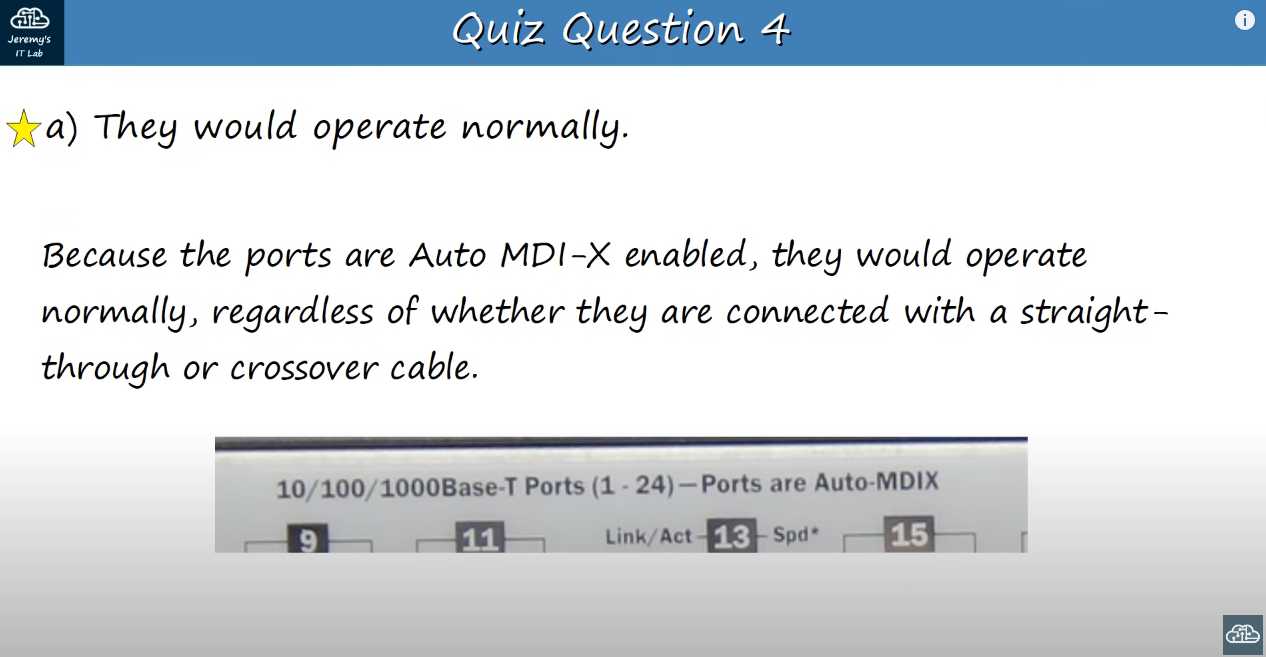
And when we want to send data between router and pc, then both of them uses 1 and 2 pin for transferring data so we have to do crossover here.

Note: UTP only covers about 100m



These 8 wires are used for larger networks.





**DAY-3**

A network protocols are the set of rules defining how network devices and software should work.

Networking models categorize and provide a structure for networking protocols and standards.

OSI Model (Open system interconnection)

* Application – Brave, chrome. Http and https are layer 7 protocols.
* Presentation – Its job is to translate between application and network formats. For example, encryption of data as it sent, and decryption of data as it is received.
* Session – Controls session between communicating hosts. Establishes, manages and terminates connections between the local application (for example, web browser) and the remote application (for example, Youtube).
* Transport – Breaks large pieces of data into smaller segments which can be more easily sent over the network and are less likely to cause transmission problems if errors occur. Layer4 header is added to each in the segmented data (smaller pieces).
* Network – Provides connectivity between end hosts on different networks. (outside of LAN). Provides path selection between source and destination. Routers operate at layer 3. Source and Destination IP address are added to the segments and are called packets.
* Data Link – In this the header and trailer (head and tail) are added and is called frame. Provides node-to-node connectivity and data transfer (for example, PC to switch, switch to router, router to router). Defines how data is formatted for transmission over a physical medium (for example, copper UTP cables). Detects and (possibly) corrects Physical Layer errors. Switches operate at layer 2.
* Physical – Defines physical characteristics of the medium used to transfer data between devices. Foe example, voltage levels, maximum transmission distances, physical connectors, cable specifications etc. Digital bits are converted into electrical (for wired connectors) or radio (for wireless connections) signals.

Note: Data, Segment, Packet and Frame are the Protocol Data Units (PDUs)

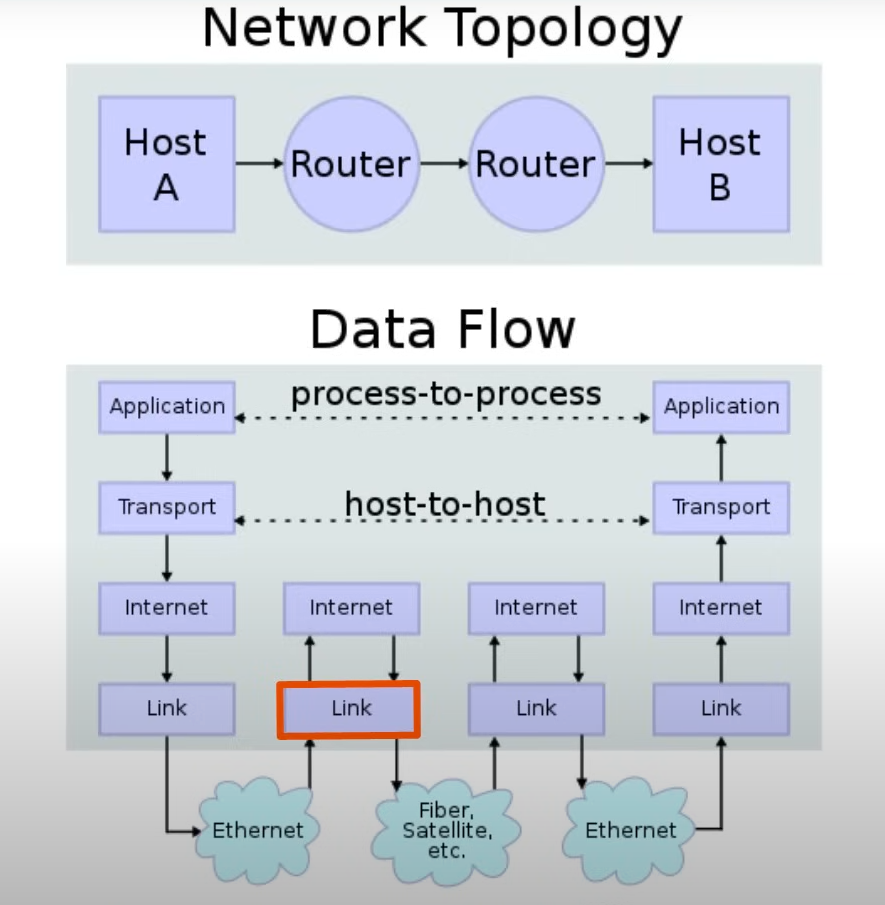
TCP/IP suite

4. Application Layer

3.Transport layer

2.Internet Layer

1. Link layer

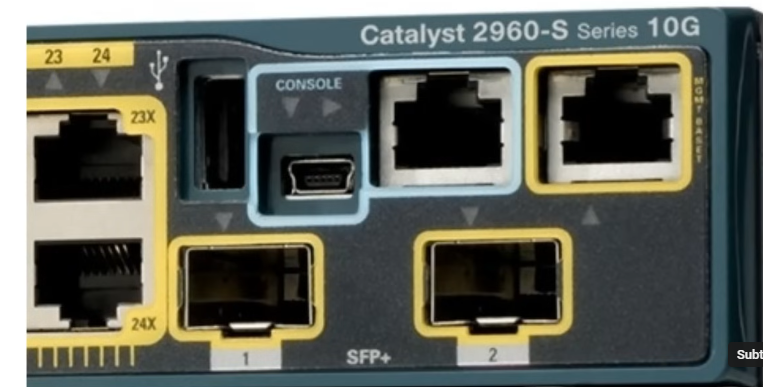


In this picture, The router is used in layer 3 as they are layer 3 devices so they want to know the ip address (source and destination) where to forward data next.

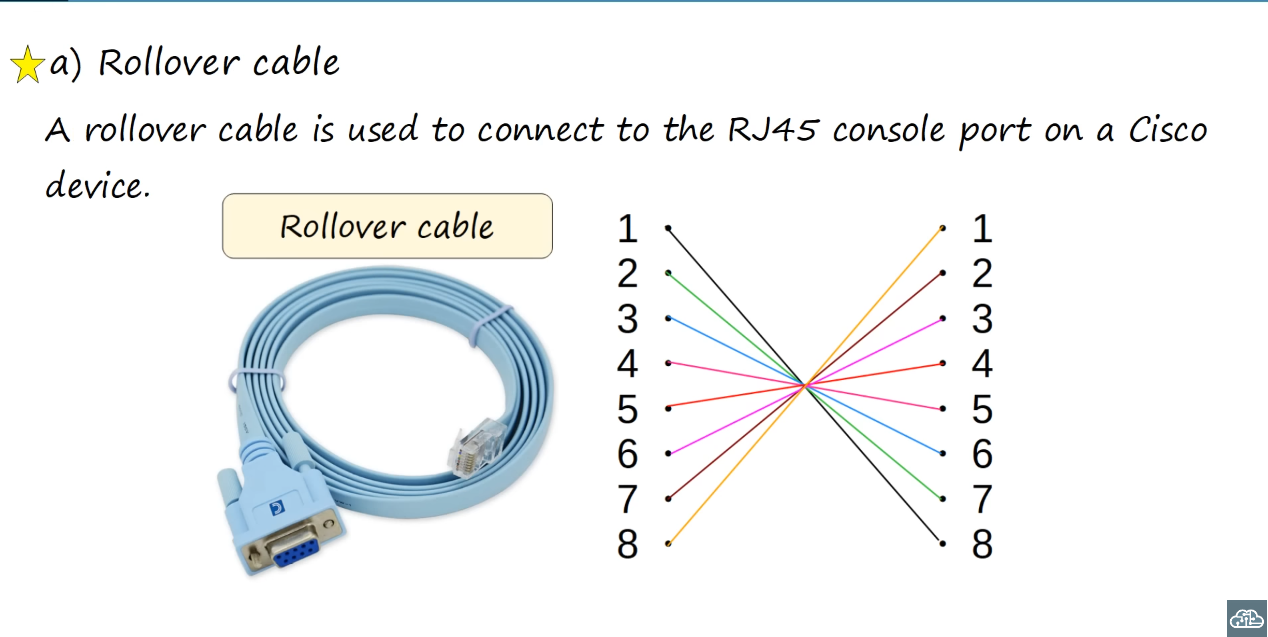
**Day-4**

CLI – Command Line Interface

How to connect to a cisco device?



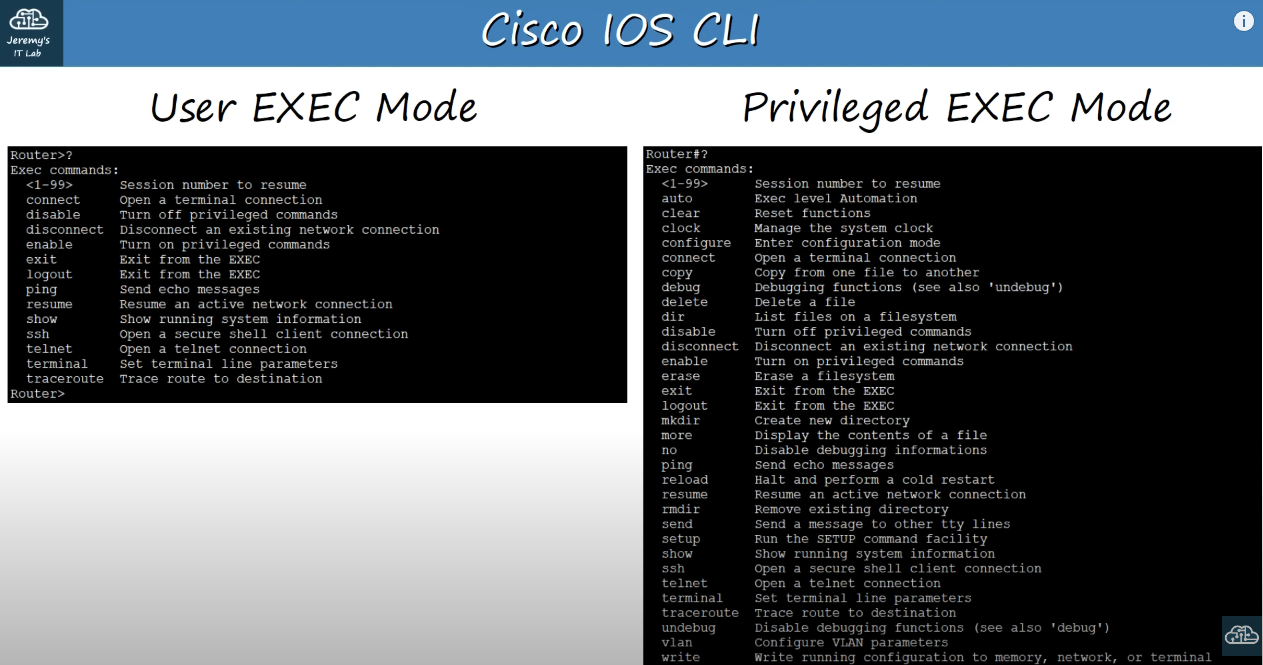
We can connect using console either using RJ45 using rollover cable or USB Mini-B



COMMANDS FOR ROUTER

1. When you first enter the CLI, you will be on User EXEC Mode. (Router>)
2. If you enter enable command, then you will be on the privileged EXEC mode. (#)

* The privileged mode provides complete access to view the devices configuration, restart the device etc.
* Cannot change the configuration, but can change the time on the device, save configuration file etc.



1. You can use (?) to view the commands that you can do.
2. To configure the terminal we have configure terminal command.
3. To set password type enable password CCNA . Here CCNA is password.
4. To save the configuration we have to type write or write memory.
5. Note to use enable secret Cisco command to secure the password.

There are two separate configuration files kept on the device at once.

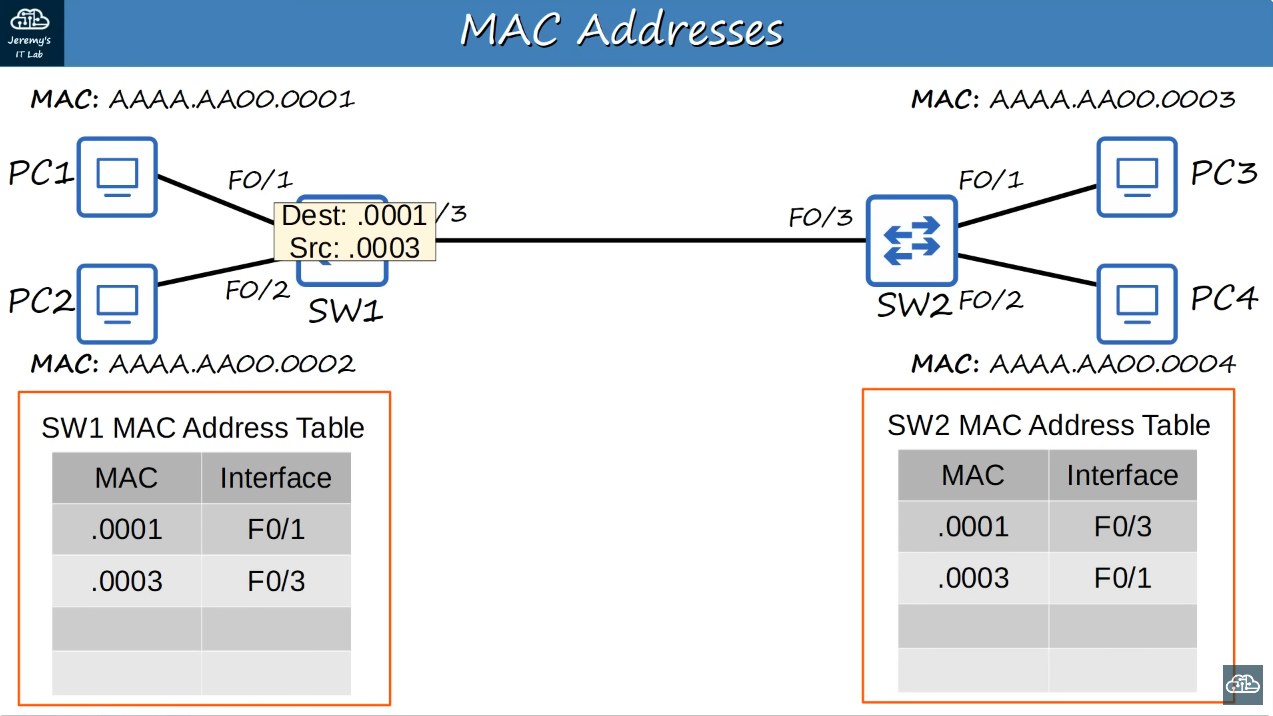
* Running-config = the current, active configuration file on the device. As you enter commands in the CLI, you edit the active configuration.
* Start-up config = the configuration file that will be loaded upon restart of the device.
* We can use the do show running-config to view and do show startup-config.
* After saving the configuration and type the show startup-config command. The password can be seen.
* So for that, we can use command service password-encryption .
* Or for better security we can use enable secret Cisco command to make the password encrypted in MD5. Cisco is the password you are using.
* If you enable service password-encryption

1. Current passwords will be encrypted.
2. Future password will be encrypted.
3. The enable secret will not be affected.

* If you disable service password-encryption using no-service password-encryption.

1. Current passwords will not be decrypted.
2. Future passwords will not be encrypted.
3. The enable secret will not be effected.

**Day-5**



The MAC address is stored only from the source, not of destination. If there is no MAC interface in the table, it will send to all other interfaces (flood) which is known as unknown unicast.

Example: What is the OUI of this MAC address? E8BA.7011.2874

* The OUI (Organizationally Unique Identifier) is the first half (24 bits) of a MAC address. It is a unique value assigned to the maker of the device.
* Answer id E8BA.70